UNIVERSITY OF OREGON

Policy Concept Form

As part of the University of Oregon Policy development process, all new Policy proposals, as well as proposals for the revision or repeal of existing Policies, must be submitted via this form to the University Secretary (the policy custodian). The Secretary will forward completed concept forms to the President's Policy Advisory Council for consideration pursuant to the University's Policy on University Policies. Please remember:

> A "Policy" as defined by the University Policy on Policies (1) has broad application or impact throughout the University community, (2) must be implemented to ensure compliance with state or federal law, (3) is necessary to enhance the University's mission, to ensure institutional consistency and operational efficiency, or to mitigate institutional risks; or (4) is otherwise designated by the Board or the President as a University Policy subject to the Policy-Making Process authorized in Section 4. A policy establishes rights, requirements or responsibilities. Excluded from this definition are things such as, but not limited to, implementation guides, operating guidelines, internal procedures, and similar management controls and tools.

[Complete the following information as thoroughly as possible; response boxes will expand as filled.]

CONCEPT SUBMITTED BY:

NAME:	José A. Domínguez
PHONE:	(541) 346-1685
EMAIL:	ciso@uoregon.edu
ORGANIZATION:	Information Services

POLICY CONCEPT SUBJECT MATTER (including existing policy number if appropriate):

Creating an Acceptable Use Policy for the University of Oregon. Today we make use of two documents created by the Oregon Department of Administrative Services before the University of Oregon created its own Board of Trustees. These are:

https://service.uoregon.edu/TDClient/2030/Portal/KB/ArticleDet?ID=30997
https://service.uoregon.edu/TDClient/2030/Portal/KB/ArticleDet?ID=30999

This new policy will complement existing policies associated with information security of university operations and assets:

https://policies.uoregon.edu/vol-4-finance-administration-infrastructure/ch-6-information-technology/information-security-program
https://policies.uoregon.edu/vol-4-finance-administration-infrastructure/ch-6-information-technology/information-asset

STATEMENT OF NEED FOR THIS POLICY CONCEPT (i.e. What is the problem this concept seeks to address, and how does this proposal do so?):

The university has been using an outdated Acceptable Use Policy to guide how university computing resources should be use and what is appropriate and inappropriate behavior while using these resources.

This policy looks to rectify this situation and create a document that is based in a set of principles rather than just dictate specific inappropriate actions that over time might become obsolete or irrelevant.

WHO OR WHAT MIGHT BE AFFECTED BY THIS POLICY CONCEPT, AND HOW? ***List all individuals, groups, etc. that would be impacted by this concept and the nature of any possible impacts (both positive and negative).***

This policy applies to all users of, and governs all use of, UO Computing Resources owned by or in the custody of the University of Oregon, including employees, students, contractors, partners, vendors, visiting scholars, and other campus visitors and guests.

This policy applies to technology, whether administered in individual departments and divisions or by central administrative departments. It also applies to all personally owned computers and devices, including mobile computing devices (e.g., smartphones, tablets, laptops, etc.), connected by wire or wirelessly to the university's network or systems, containing legally restricted information (e.g., pictures, medical information, other protected information, etc.) and to off-site computers that connect remotely to network services.

WHAT COSTS MIGHT BE ASSOCIATED WITH THIS CONCEPT, BOTH IMPLEMENTATION AND RECURRING?

There are no immediate costs associated with enacting this policy.

WHAT OTHER RESOURCES (HUMAN, PHYSICAL, OPERATIONAL, FINANCIAL, TECHNOLOGICAL, ETC.), WILL BE NEEDED TO IMPLEMENT AND MAINTAIN COMPLIANCE WITH THIS POLICY?

Operational implementation of the policy won't change current processes but standardizes them into formal policy.

Information Services, Informations Security Office and IT staff perform most of the tasks necessary as part of their jobs.

Human Resources, the Dean of Students, Office of General Counsel already ar e involved when there are violations to the current outdated policy.

DOES THE PROPOSED CONCEPT IMPACT EXISTING POLICIES, GUIDELINES OR PROCEDURES? DOES THE PROPOSED CONCEPT RELATE TO A MATTER WITHIN A UNION CONTRACT? IF SO, PLEASE LIST.

The policy will replace:
https://service.uoregon.edu/TDClient/2030/Portal/KB/ArticleDet?ID=30997
https://service.uoregon.edu/TDClient/2030/Portal/KB/ArticleDet?ID=30999

Beyond that, we were not made aware of impact to other policies, guidelines or procedures during conversations with stakeholders.

ADDITIONAL INFORMATION YOU WISH TO SHARE?

No additional information.

PLEASE PROVIDE ANY SUGGESTED LANGUAGE AS AN ATTACHMENT TO THIS FORM.

FOR OFFICE USE ONLY

Date Received:

POLICY CONCEPTS: INSTRUCTIONS AND GUIDELINES

All policy proposals – including new policy concepts, proposed revisions, or suggested repeals – must be submitted via the form on page 2 to the Office of the University Secretary with appropriate supporting information and documents. Completed submissions are forwarded to the University Senate (academic policies) or the President's Policy Advisory Council (PAC), which ensures proper routing through the policy-making process. (See UO Policy I.03.01 for more information.)

Please keep the following definition of a university policy in mind as you develop your concept:

> *A University Policy ("Policy") is a policy that (1) has broad application or impact throughout the University community, (2) must be implemented to ensure compliance with state or federal law, (3) is necessary to enhance the University's mission, to ensure institutional consistency and operational efficiency, or to mitigate institutional risks; or (4) is otherwise designated by the Board [of Trustees] or the President [of the University] as a University Policy.*
>
> *A policy establishes rights, requirements or responsibilities. Excluded from this definition are things such as, but not limited to, implementation guides, operating guidelines, internal procedures, and similar management controls and tools.*

To help facilitate as smooth a process as possible, please consider the following:

1. Consult as many stakeholders as possible *prior to submitting* your concept. A primary role for the PAC is to ensure that appropriate offices, departments or groups are consulted.

2. Run your concept by the Office of General Counsel (OGC) *prior to submission*. OGC review is a required step in policy-making.

3. Please use the proper template – email uopolicy@uoregon.edu to obtain either (a) the new policy template (new proposals) or (b) the Word version of the existing policy in its proper template (for redlines/revisions).

4. A "redlined" version of your concept in Word is required for proposed revisions. This must be done using the appropriate Word version (see #3, above).

5. Include any appropriate related resources that will be useful to those reviewing the concept. Links are preferred, but supplemental documents are of course acceptable for items not online. Examples of such items include any associated procedures or unit level policies (even if in draft form), or other policies or procedures related to, overridden by, necessary as a result of, or otherwise affiliated with your concept;

6. Please submit all documents as individual files.

7. Someone from the responsible office or proposing unit will need to attend a PAC meeting to explain the concept and answer any questions.

Please email uopolicy@uoregon.edu if you have any questions. Thank you!

POLICY CONCEPT FORM

Name and UO Title/Affiliation:	José A. Domínguez, Chief Information Security Officer
Policy Title & # (if applicable):	Acceptable Use Policy
Submitted on Behalf Of:	Self
Responsible Executive Officer:	Jammie Moffitt, Senior Vice President for Finance and Administration/CFO

SELECT ONE: ☒ **New Policy** ☐ **Revision** ☐ **Repeal**
Click the box to select

HAS THE OFFICE OF GENERAL COUNSEL REVIEWED THIS CONCEPT: ☒ **Yes** ☐ **No**
If yes, which attorney(s): Ryan Hegemann

GENERAL SUBJECT MATTER
Include the policy name and number of any existing policies associated with this concept.

This new policy will complement existing policies associated with information security of university operations and assets:

https://policies.uoregon.edu/vol-4-finance-administration-infrastructure/ch-6-information-technology/information-security-program
https://policies.uoregon.edu/vol-4-finance-administration-infrastructure/ch-6-information-technology/information-asset

---

RELATED STATUTES, REGULATIONS, POLICIES, ETC.
List known statutes, regulations, policies (including unit level policies), or similar related to or impacted by the concept. Include hyperlinks where possible, excerpts when practical (e.g. a short statute), or attachments if necessary. Examples: statute that negates the need for or requires updates to an existing policy; unit level policy(ies) proposed for University-wide enactment; or existing policies used in a new, merged and updated policy.

Creating an Acceptable Use Policy for the University of Oregon. Today we make use of two documents created by the Oregon Department of Administrative Services before the University of Oregon created its own Board of Trustees. These are:

https://service.uoregon.edu/TDClient/2030/Portal/KB/ArticleDet?ID=30997
https://service.uoregon.edu/TDClient/2030/Portal/KB/ArticleDet?ID=30999

STATEMENT OF NEED

What does this concept accomplish and why is it necessary?

In support of our commitment to exceptional teaching, discovery, and service, the University of Oregon ("UO") provides access to its network, information, and other computing resources to the UO community and guests. These resources are provided to empower excellence in instruction, research, and service by facilitating academic inquiry, communication, sharing, collaboration, and effective administration while protecting user safety, privacy, and supporting academic freedom in a secure and resilient environment. Maintaining this environment requires that members of the UO community, visitors, and guests respect the rights of other users, use resources responsibly, and endeavor to defend our computing resources. The purpose of this policy is to establish acceptable behavior and promote efficient, ethical, and legal use of UO's Computing Resources.

AFFECTED PARTIES

Who is impacted by this change, and how?

This policy applies to all users of, and governs all use of, UO Computing Resources owned by or in the custody of the University of Oregon, including employees, students, contractors, partners, vendors, visiting scholars, and other campus visitors and guests.

This policy applies to technology, whether administered in individual departments and divisions or by central administrative departments. It also applies to all personally owned computers and devices, including mobile computing devices (e.g., smartphones, tablets, laptops, etc.), connected by wire or wirelessly to the university's network or systems, containing legally restricted information (e.g., pictures, medical information, other protected information, etc.) and to off-site computers that connect remotely to network services.

CONSULTED STAKEHOLDERS

Which offices/departments have reviewed your concept and are they confirmed as supportive? (Please do not provide a list of every individual consulted. Remain focused on stakeholders (e.g. ASUO, Office of the Provost, Registrar, Title IX Coordinator, etc.).)

Name	Office	Date

SEE APPENDIX A FOR LIST OF STAKEHOLDERS CONSULTED. WHEN SEVERAL INDIVIDUALS WERE CONSULTED, THE WORD "MULTIPLE" WAS USED UNDER THE NAME HEADING.

APPENDIX A – STAKEHOLDERS CONSULTED

Name	Office	Dates Contacted
Multiple	Audit Office	January 2023, May 2025
Multiple	Business Affairs	September 2021, April 2025
Multiple	Clark Honors College	April-May 2025
Multiple	College of Arts & Science	April-May 2025
Multiple	College of Design	April-May 2025
Multiple	College of Education	April-May 2025
Multiple	Division of Equity & Inclusion	April-May 2025
Multiple	Division of Global Engagement	April-May 2025
Multiple	Division of Student Life	January 2022, May 2025
Multiple	Finance & Administration	Sept. 2022, May 2025
Multiple	General Counsel	January 2022 through May 2025
Multiple	Human Resources	January, 2022, May 2025
Multiple	Information Services	September 2022, January 2023, May 2025
Multiple	Intercollegiate Athletics	April-May 2025
Multiple	Knight Campus	April-May 2025
Multiple	Lundquist College of Business	April-May 2025
Kassy Fisher	Office of the President	May 2025
Multiple	Office of the Provost	Sept. 2022, May 2025
Mahnaz Ghaznavi	Public Records Office	March 2023
Multiple	Research & Innovation	June 2021, April 2023, May 2025
Multiple	Safety and Risk Services	April-May 2025
Multiple	School of Journalism and Communications	April-May 2025
Multiple	School of Law	April-May 2025
Multiple	School of Music and Dance	April-May 2025
Multiple	Student Services & Enrollment Management	April-May 2025
Multiple	University Advancement	April-May 2025
Multiple	University Communications	April-May 2025
Multiple	University Health Services	September 2022, May 2025
Multiple	University Library	May 2021, May 2025
Multiple	University Senate	January 2022, October 2023, May 2025
Multiple	UO Portland	April-May 2025

Reason for Policy

This policy establishes the acceptable, as well as unacceptable or unauthorized, use of University of Oregon Computing Resources by all Users, internal or external.

Entities Affected by this Policy

All Users, internal or external, of University of Oregon Computing Resources.

Web Site Address for this Policy

[Provided by Office of the University Secretary after policy is posted online]

Responsible Office

For questions about this policy, please contact the Office of the Chief Information Security Officer, (541) 346-1701, or ciso@uoregon.edu.

Enactment & Revision History

Day-Month-Year – [text]
Day-Month-Year – [text]

Definitions

Artificial Intelligence (AI) refers to a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

Data refers to raw, unprocessed text, facts or figures that lack context on their own. [*In this document, data and information might be used interchangeably*].

Data Availability refers to methods for ensuring that required data is always accessible when needed, in accordance with university retention policies.

Data Confidentiality refers to methods for ensuring that access to sensitive data is limited to authorized individuals.

Data Integrity refers to methods for ensuring that data is complete, accurate, consistent, and safeguarded from unauthorized modification.

Information is data that has been organized, interpreted, and given context to become meaningful and useful for decision-making; essentially, information is processed data that provides insights and understanding. [*In this document, data and information might be used interchangeably*].

Large Language Model (LLM) refers to powerful machine learning or Artificial Intelligence (AI) algorithms that can generate human-like text, understand natural language, trained on massive datasets of text and are designed to predict the next word in a sequence, allowing them to perform tasks like translation, summarization, and content generation.

University of Oregon (UO) Computing Resources means university-owned, licensed or managed data stored in any form (e.g., electronic, paper, or any other medium), hardware (e.g., central processing unit, computer memory and peripherals, file storage, Internet of things devices), software, network infrastructure, Internet Protocol (IP) addresses, email accounts, and domain names, regardless of location, whether on-premises, in the cloud or elsewhere.

University of Oregon (UO) Records means any record as defined in the university records management policy IV.10.01.

User (of UO Computing Resources) means any individual who attempts to access or has access to UO Computing Resources.

Policy

Purpose

In support of our commitment to exceptional teaching, discovery, and service, the University of Oregon ("UO") provides access to its network, information, and other computing resources to the UO community and guests. These resources are provided to empower excellence in instruction, research, and service by facilitating academic inquiry, communication, sharing, collaboration, and effective administration and operations while protecting User safety and privacy, and supporting academic freedom in a secure and resilient environment. Maintaining this environment requires that members of the UO community, visitors, and guests respect the rights of other Users, use resources responsibly, and endeavor to defend our computing resources. The purpose of this policy is to establish acceptable behavior and promote efficient, ethical, and legal use of UO Computing Resources.

Scope

This policy applies to all Users of, and governs all use of, UO Computing Resources owned by or in the custody of the University of Oregon, including employees, students, contractors, partners, vendors, visiting scholars, and other campus visitors and guests.

This policy applies to technology whether administered in individual departments and divisions or by central administrative departments. It also applies to non-university devices, including personally owned computers and devices such as mobile computing devices (e.g., smartphones, tablets, laptops), which are connected by wire or wirelessly to the university's network or systems, devices containing legally restricted university information (e.g., pictures, medical information, other protected information), and off-site systems that connect remotely to university network services.

Access to UO Computing Resources must comply with this policy, all other applicable university policies, procedures, established practices, and state and federal laws.

Rights and Responsibilities

The university provides Users with access to scholarly and/or work-related technologies and tools, as well as access to computing resources, including but not limited to computer systems, servers, software and databases, to the campus telephone and voice mail systems, the library system, and to the Internet and cloud online services. Users have a reasonable expectation of unobstructed use of these resources available to them, of certain degrees of privacy (which may vary depending on whether the User is a

university employee or a prospective or enrolled student), and of protection from abuse and intrusion by others sharing these resources. Users can expect the right to access information and to express their opinion to be protected as it is for paper and other forms of non-electronic communication.
Conversely, Users are responsible for knowing the regulations and policies of the university that apply to appropriate and acceptable use of the UO Computing Resources. Users are responsible for exercising good judgment in the use of the university's technological and information resources.
By using UO computing resources, and/or accepting any UO-issued computing accounts, the User agrees to comply with this and all other computing and information security-related policies. Users have the responsibility to keep up to date on changes in the computing environment, as published, using UO electronic and print publication mechanisms, and to adapt to those changes as necessary.

Principles

The requirements for acceptable use of UO Computing Resources outlined in this policy are guided by the following general principles:

1. UO Computing Resources are intended to enable the university's research, instructional, administrative, and service-related functions. Uses within and beyond these functions must comply with existing university policies and procedures as well as state and federal law.
2. UO Computing Resources are to be used and supported to ensure data confidentiality, integrity, and availability.
3. Each User is expected to comply with UO Information Security policies and standards, and take necessary precautions as outlined in UO Information Security policies, standards, and guidelines to ***safeguard*** UO Computing Resources and to report policy violations or suspected security incidents.
4. Each User is expected to use UO Computing Resources ***responsibly*** and to be ***considerate*** of other Users of shared resources.
5. Subject to law and applicable policy, ***authorized university personnel with a demonstrably legitimate need may access an individual's specific UO Computing Resources*** to fulfill their official professional responsibilities (e.g., conducting security incident investigations by IT staff). See "Access and Review" below.

Expectations for Appropriate Use

The following statements are examples that illustrate expectations for acceptable use of UO Computing Resources based on the principles outlined above. They are not meant to be an exhaustive list of all possible expectations that govern the use of UO Computing Resources. The Information Security Office maintains a Catalog of Appropriate and Acceptable Use of Computing Resources findings pertinent to the Acceptable Use Policy. Users are responsible for reviewing the catalog for current findings.

A. **Use UO Computing Resources to perform activities that support the research, instruction, service, administration, and other goals of the university**. Incidental personal use is permitted but is required to comply with university policies and standards, meet legal requirements, and not interfere with or disrupt university operations.
B. **Safeguard UO Computing Resources in accordance with policies, standards, and guidelines established by the university**. As a **U**ser of UO Computing Resources, **U**sers may be provided

with computer access accounts, computing devices, access to the network, email accounts and other resources. Protect all personally identifiable information (PII), protected health information (PHI) and other sensitive data in accordance with applicable data privacy regulations (e.g., UO Privacy Policy, FERPA, HIPAA, GDPR, Oregon Consumer Privacy Act, California Privacy Rights Act). Users must take steps to increase their knowledge through UO security awareness training and follow UO policies, standards, and guidelines to properly safeguard these resources.

C. **Use UO Computing Resources after proper authorization has been granted**. Generally, access is granted to UO Users based on two security principles: 1) *least privilege*, where the minimum privilege required to carry out approved activities is assigned to each User; 2) *least functionality*, where UO Computing Resources are configured to provide Users with the minimum functionality required to carry out their duties.
D. **Use UO Computing Resources in a responsible and efficient manner**. UO Computing Resources (e.g., network bandwidth, storage, email system, and computer processing power) are finite and usually shared among our constituents. Therefore, Users are expected to use resources in a manner that minimizes impacts on other Users.
E. **Respect the privacy, intellectual property, copyrights and other rights of other UO Computing Resource Users**. Academic inquiry, communication, sharing and collaboration, IT management and support, and information security must be balanced with privacy and other rights of UO constituents and must not improperly or illegally infringe on the intellectual property rights of others.
F. **Use UO Computing Resources in accordance with policies, standards, and guidelines established by the university such as the Conflict of Interest, Conflict of Commitment, and Outside Activities policy, and in accordance with bargaining agreements, state and federal laws, and contractual agreements**. As a User of UO Computing Resources, Users may be provided with computer access accounts, computing devices, access to the network, email accounts and other resources. Users must take steps to increase their knowledge through UO security awareness training and follow UO policies, standards and guidelines to properly safeguard these resources.
G. **Use and protect UO Computing Resources assigned to you**. As part of their affiliation with the university, Users may be assigned IT resources (e.g., computer access account, email account, network port, computers, office phone, peripherals, and mobile devices). Users are expected to bear responsibility for and may be held accountable for actions carried out with those resources.
H. **Include only material relevant to organizational matters in UO or departmental electronic communications, such as email, websites, or blogs.** Personal websites, chat rooms, web logs (also known as blogs), video logs (also known as vlogs), and other forms of publicly available electronic communications hosted on or linked from UO computing resources and technology must comply with this Acceptable Use Policy and prominently include the following disclaimer: "***The views, opinions and material expressed here are those of the author and have not been reviewed or approved by the University of Oregon.***"
I. **Use only legal versions of copyrighted software in compliance with vendor license requirements**. Abide by all applicable copyright laws and licenses. The University of Oregon has

entered into legal agreements or contracts for many of its software and network resources which require everyone using them to comply with those agreements.

J. **Maintain university data and records within authorized information systems of record and in compliance with appropriate records retention policies**. The university cannot guarantee appropriate safeguards for data or information hosted in information systems that have not been approved. Consequently, Users are expected to maintain university data and records within information systems that have been vetted and approved by the university. For example, use of unapproved third-party email systems, storage solutions or applications must be vetted and approved by the Information Security Office before such systems can be used to access, process or store University Records and data (e.g., follow guidelines on where to store UO data).

Examples of Inappropriate Use or Misuse

The following are examples of inappropriate use or misuse of UO Computing Resources. This list is meant to illustrate common misuse and is not intended to be an exhaustive list. Some activities will not be considered inappropriate use or misuse when authorized by appropriate UO officials (e.g., when testing effectiveness and performance of security safeguards or when performing one's duties). The Information Security Office maintains a Catalog of Inappropriate and Unacceptable Use of Computing Resources findings pertinent to the Acceptable Use Policy. Users are responsible for reviewing the catalog for current findings.

A. Searching for and attempting to circumvent or exploit information system security flaws in UO Computing Resources without the express permission of the Information Security Office (e.g., using tools such as vulnerability scanners, penetration testing, password crackers, packet sniffers, social engineering techniques such as phishing, or other hacking tools).
B. Performing intentional and/or malicious excessive use of UO Computing Resources that substantially interferes with the university's mission.
C. Sharing your personal, or individual non-person, account access credentials such as passwords or tokens with another person, including but not limited to your IT support staff, Information Security Office staff, supervisors, your staff, family or friends.
D. Storing or processing UO data in information systems that do not comply with university security policies, standards, and controls or that violate applicable regulatory requirements.
E. Attempting to impersonate, intercept, alter, or monitor another User's communications or files without their permission or an approved business need.
F. Taking deliberate actions that significantly disrupt university operations, violate confidentiality agreements, or significantly increase the risk of causing a security incident.
G. Attempting to locate data on UO Computing Resources for which the User does not possess a justifiable business reason for attempting access. Technical ability to access data does not automatically confer authorization to access said data without a valid business justification. Attempts to access data may include, but are not limited to, the following:
    a. Navigating accessible SharePoint sites and file shares.
    b. Searching SharePoint sites.
    c. Searching messaging tools (e.g., Slack or Teams) for data.
    d. Using AI assistants (e.g., Microsoft Copilot) to locate data.

    e. Querying databases and other structured/semi-structured data stores for data.

H. Using email, social networking sites or tools, text messaging (SMS, video, picture, audio or other media messaging provided via mobile phone) or other messaging services in any inappropriate manner including, but not limited to, usage:
    a. In violation of laws or regulations.
    b. To harass or intimidate another person.
    c. To display sensitive information covered under security and privacy policies and standards.
I. Using UO Computing Resources to gain unauthorized access to, or in any way compromise the security of, any UO or non-UO person, computer systems or services.
J. Using UO Computing Resources to violate UO policies, standards and guidelines, state and federal laws, and contractual agreements.

Enforcement

This policy has the force of law pursuant to ORS 352.087. A university employee who fails to comply with this policy and its associated procedures may be subject to discipline, up to and including termination. Discipline will be imposed consistent with applicable university policies and/or applicable collective bargaining agreements. A student who fails to comply with this policy and its associated procedures may be referred to the Office of Student Conduct and Community Standards for educational intervention and subject to action and/or sanction as outlined by the Student Conduct Code. Contractors, partners, vendors, visiting scholars, and other campus visitors and guests in violation of this policy and its associated procedures might have their access to UO Computing Resources modified, suspended, or terminated depending on the violation. In some cases, violations of this policy may also constitute violations of state and federal laws and include associated consequences.

Unintended minor violations or accidental infractions will typically result in warnings, notifications, or recommendations for awareness training. In addition, students involved in unintended minor violations or accidental infractions may be referred to the Office of Student Conduct and Community Standards for educational intervention.

Instances where network and other hardware devices, computer systems, applications, data or information, access accounts or other components are found to be in violation of UO policies, standards, or procedures, defensive actions may be taken by authorized UO staff such as the Information Security Office to safeguard UO Computing Resources and protect other Users. Examples of defensive actions may include removal or blocking of applications, websites, or devices from the network, disabling access accounts, or other measures as appropriate to mitigate the specific risk.

Access and Review

Because the university owns, controls, and has a custodial relationship with its Computing Resources, it reserves the right to monitor usage of those resources to ensure their security, availability, efficiency, and effectiveness. This access and review will be consistent with state and federal law, collective bargaining agreements and with other university policies and procedures. A non-exhaustive list of examples of specific circumstances under which monitoring and/or access can be carried out, by authorized personnel, includes:

- to investigate potential violations of UO policy, standards, guidelines, or state, federal laws or contractual agreements
- to comply with legal requests, including public records laws and subpoenas
- to perform authorized security functions including audits, risk identification, incident prevention, threat and vulnerability monitoring, misuse investigation, incident response or patch management
- to access information in case of emergencies to protect the health and safety of individuals and safeguard university-owned or controlled assets, if deemed necessary by authorized personnel
- to perform administration of UO Computing Resources in accordance with UO policies, standards and procedures or generally accepted industry best practices.
- to access electronic records to ensure the continuous operation of university business and mission.

Reporting Misuse

Suspected misuse of UO Computing Resources, or violations of this policy and underlying standards and procedures must be reported to the UO Information Security Office by emailing infosec@uoregon.edu or by calling (541) 346-5837. Alternately, suspected misuse can be reported to the Office of Internal Audit (OIA) either directly (541-346-3200) or through the anonymous and confidential Fraud & Ethics Hotline available from the OIA intranet page.

Exception

In a limited number of instances, exceptions to parts of this policy may be granted. In these cases, an exception request should be submitted to the Information Security Office, outlining justification for the request. The exception request procedure and request form are outlined in Information Security Standard Exception Request.

Related Resources

Catalog of Appropriate and Acceptable Use of Computing Resources
Catalog of Inappropriate and Unacceptable Use of Computing Resources
Information Security Program Policy
Information Asset Classification & Management Policy
Data Security Incident Response Policy

Catalog of Appropriate & Acceptable Use of Computing Resources

The University of Oregon has an Acceptable Use Policy (AUP). The requirements for acceptable use of UO Computing Resources outlined in the AUP are guided by the following general principles:

1. UO Computing Resources are intended to enable the university's research, instructional, administrative, and service-related functions. Uses beyond these functions must comply with existing university policies and procedures as well as state and federal law.
2. UO Computing Resources are to be used and supported to ensure data confidentiality, integrity, and availability.
3. Each user is expected to comply with UO Information Security policies and standards; and take necessary precautions as outlined in UO Information Security policies, standards, and guidelines to ***safeguard*** UO Computing Resources and to report policy violations or suspected security incidents.
4. Each user is expected to use UO Computing Resources ***responsibly*** and to be ***considerate*** of other users of shared resources.
5. Subject to law and applicable policy, ***authorized university personnel with a demonstrably legitimate need may access an individual's specific UO Computing Resources*** to fulfill their official professional responsibilities (e.g., conducting security incident investigations by IT staff). See "Access and Review" below.

The entries in this document represent events, actions or behaviors that comply with the appropriate and acceptable use of UO Computing Resources.

As the university encounters new situations that require an evaluation as to whether they are in accordance with the principles stated above, the Information Security Office (ISO) staff and the Information Security and Privacy Governance Subcommittee (ISP-GC) will review the merits and render a decision. If the evaluation finds them acceptable, they will be logged into this document and tagged with the date of the finding. This analysis will not preclude the university from acting promptly to ensure the protection of the confidentiality, integrity, and availability of university data and computing resources.

If the analysis finds the action to be in violation of the principles of the AUP, it will be logged into the Catalog of Inappropriate & Unacceptable Use of Computing Resources.

Commented [JD1]: Convert into a hyperlink.

Entry Date	Activity Description
	Use UO Computing Resources to perform activities that support the research, instruction, service, administration, and other goals of the university. Incidental personal use is permitted but is required to comply with university policies and standards, meet legal requirements, and not interfere with or disrupt university operations.
	Safeguard UO Computing Resources in accordance with policies, standards, and guidelines established by the university. As a User of UO Computing Resources, Users may be provided with computer access accounts, computing devices, access to the network, email accounts and other resources. Protect all personally identifiable

Commented [JD2]: Entry date for these initial rows will be the day the policy comes into effect.

	information (PII), protected health information (PHI) and other sensitive data in accordance with applicable data privacy regulations (e.g., UO Privacy Policy, FERPA, HIPAA, GDPR, Oregon Consumer Privacy Act, California Privacy Rights Act). Users must take steps to increase their knowledge through UO security awareness training and follow UO policies, standards, and guidelines to properly safeguard these resources.
	Use UO Computing Resources after proper authorization has been granted. Generally, access is granted to UO Users based on two security principles: 1) *least privilege*, where the minimum privilege required to carry out approved activities is assigned to each User; 2) *least functionality*, where UO Computing Resources are configured to provide Users with the minimum functionality required to carry out their duties.
	Use UO Computing Resources in a responsible and efficient manner. UO Computing Resources (e.g., network bandwidth, storage, email system, and computer processing power) are finite and usually shared among our constituents. Therefore, Users are expected to use resources in a manner that minimizes impacts on other Users.
	Respect the privacy, intellectual property, copyrights and other rights of other UO Computing Resource Users. Academic inquiry, communication, sharing and collaboration, IT management and support, and information security must be balanced with privacy and other rights of UO constituents and must not improperly or illegally infringe on the intellectual property rights of others.
	Use UO Computing Resources in accordance with policies, standards, and guidelines established by the university such as the Conflict of Interest, Conflict of Commitment, and Outside Activities policy, and in accordance with bargaining agreements, state and federal laws, and contractual agreements. As a User of UO Computing Resources, Users may be provided with computer access accounts, computing devices, access to the network, email accounts and other resources. Users must take steps to increase their knowledge through UO security awareness training and follow UO policies, standards and guidelines to properly safeguard these resources.
	Use and protect UO Computing Resources assigned to you. As part of their affiliation with the university, Users may be assigned IT resources (e.g., computer access account, email account, network port, computers, office phone, peripherals, and mobile devices). Users are expected to bear responsibility for and may be held accountable for actions carried out with those resources.
	Include only material relevant to organizational matters in UO or departmental electronic communications, such as email, websites, or blogs. Personal websites, chat rooms, web logs (also known as blogs), video logs (also known as vlogs), and other forms of publicly available electronic communications hosted on or linked from UO computing resources and technology must comply with this Acceptable Use Policy and prominently include the following disclaimer: "*The views, opinions and material expressed here are those of the author and have not been reviewed or approved by the University of Oregon*."
	Use only legal versions of copyrighted software in compliance with vendor license requirements. Abide by all applicable copyright laws and licenses. The University of Oregon has entered into legal agreements or contracts for many of its software and

	network resources which require everyone using them to comply with those agreements.
	Maintain university data and records within authorized information systems of record and in compliance with appropriate records retention policies. The university cannot guarantee appropriate safeguards for data or information hosted in information systems that have not been approved. Consequently, Users are expected to maintain university data and records within information systems that have been vetted and approved by the university. For example, use of unapproved third-party email systems, storage solutions or applications must be vetted and approved by the Information Security Office before such systems can be used to access, process or store University Records and data (e.g., follow guidelines on where to store UO data).
	While UO Computing Resources are to be used predominantly for university-related business, personal use is permitted so long as it conforms with this Policy and does not interfere with university operations or an employed User's performance of duties as a university employee. As with permitted personal use of other resources, limited personal use of UO Computing Resources does not ordinarily result in additional costs to the university and may result in increased efficiencies.
	Protect all personally identifiable information (PII), protected health information (PHI) and other sensitive data in accordance with applicable data privacy regulations (e.g., UO Private Policy, FERPA, HIPAA, GDPR, Oregon Consumer Privacy Act, California Privacy Rights Act, etc.).
	Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in the production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy, and copyright infringement.

Revision History

Version	Published	Author	Description
1.0		Information Security Office (ISO)	Original publication

Catalog of Inappropriate & Unacceptable Use of Computing Resources

The University of Oregon has an Acceptable Use Policy (AUP). The requirements for acceptable use of UO Computing Resources outlined in this policy are guided by the following general principles:

1. UO Computing Resources are intended to enable the university's research, instructional, administrative, and service-related functions. Uses beyond these functions must comply with existing university policies and procedures as well as state and federal law.
2. UO Computing Resources are to be used and supported to ensure data confidentiality, integrity, and availability.
3. Each user is expected to comply with UO Information Security policies and standards; and take necessary precautions as outlined in UO Information Security policies, standards, and guidelines to ***safeguard*** UO Computing Resources and to report policy violations or suspected security incidents.
4. Each user is expected to use UO Computing Resources ***responsibly*** and to be ***considerate*** of other users of shared resources.
5. Subject to law and applicable policy, ***authorized university personnel with a demonstrably legitimate need may access an individual's specific UO Computing Resources*** to fulfill their official professional responsibilities (e.g., conducting security incident investigations by IT staff). See "Access and Review" below.

The entries in this document represent events, actions or behaviors that do not comply with the appropriate and acceptable use of UO Computing Resources.

As the university encounters new situations that require an evaluation as to whether they are in accordance with the principles stated above, the Information Security Office (ISO) staff and the Information Security and Privacy Governance Subcommittee (ISP-GC) will review the merits and render a decision. If the evaluation finds them unacceptable, they will be logged into this document and tagged with the date of the finding. This analysis will not preclude the university from acting promptly to ensure the protection of the confidentiality, integrity and availability of university data and computing resources.

If the analysis finds the action follows the principles of the AUP, it will be logged into the Catalog of Appropriate & Acceptable Use of Computing Resources.

Commented [JD1]: Convert into a hyperlink.

Inappropriate & Unacceptable Use Entries

Entry Date	Activity Description
	Searching for and attempting to circumvent or exploit information system security flaws in UO Computing Resources without the express permission of the Information Security Office (e.g., using tools such as vulnerability scanners, penetration testing, password crackers, packet sniffers, social engineering techniques such as phishing, or other hacking tools).

Commented [JD2]: Entry date for these initial rows will be the day the policy comes into effect.

	Performing intentional and/or malicious excessive use of UO Computing Resources that substantially interferes with the university's mission.
	Sharing your personal, or individual non-person, account access credentials such as passwords or tokens with another person, including but not limited to your IT support staff, Information Security Office staff, supervisors, your staff, family or friends.
	Storing or processing UO data in information systems that do not comply with university security policies, standards, and controls or that violate applicable regulatory requirements.
	Attempting to impersonate, intercept, alter, or monitor another User's communications or files without their permission or an approved business need.
	Taking deliberate actions that significantly disrupt university operations, violate confidentiality agreements, or significantly increase the risk of causing a security incident.
	Attempting to locate data on UO Computing Resources for which the User does not possess a justifiable business reason for attempting access. Technical ability to access data does not automatically confer authorization to access said data without a valid business justification. Attempts to access data may include, but are not limited to, the following: a. Navigating accessible SharePoint sites and file shares. b. Searching SharePoint sites. c. Searching messaging tools (e.g., Slack or Teams) for data. d. Using AI assistants (e.g., Microsoft Copilot) to locate data. e. Querying databases and other structured/semi-structured data stores for data.
	Using email, social networking sites or tools, text messaging (SMS, video, picture, audio or other media messaging provided via mobile phone) or other messaging services in any inappropriate manner including, but not limited to, usage: a. In violation of laws or regulations. b. To harass or intimidate another person. **c.** To display sensitive information covered under security and privacy policies and standards
	Using UO Computing Resources to gain unauthorized access to, or in any way compromise the security of, any UO or non-UO person, computer systems or services.
	Using UO Computing Resources to violate UO policies, standards and guidelines, state and federal laws, and contractual agreements.
	Transmit commercial or personal advertisements, solicitations, endorsements or promotions unrelated to the business of the university or in violation of other university policies.
	Send, receive or store legally restricted and/or confidential information via means not approved by the information security office (e.g., usage of unapproved cloud-based storage).
	Access, transmit or otherwise use illicit or inappropriate material (e.g., child pornography, drug sales, etc.) through email, internet traffic or by any other means through the use of UO Computing resources.
	Knowingly introduce any computing device to the university network that is infected with malware (or suspected to be otherwise compromised).

	Using generative AI tools (e.g., ChatGPT, Gemini, Copilot, or other LLMs) to perform malicious or inappropriate actions, or to generate malicious, inappropriate or illegal material.
	Using any AI-based tools and services that have not been explicitly authorized by UO Information Services to handle UO proprietary information. Authorizations are not transferable from one user to another. Authorization for the use of AI-based services will include a combination of all the following. a. The authorized AI tool/service. b. The authorized user of the AI tool/service. c. The business use case for which the AI tool/service may be used.
	Using public cloud platforms (e.g., AWS, Microsoft Azure, etc.) to store or process university's proprietary data without explicit authorization from UO Information Services.

Revision History

Version	Published	Author	Description
1.0		Information Security Office (ISO)	Original publication