ARTICLE 39. ACCEPTABLE USE OF UNIVERSITY INFORMATION ASSETS

Section 1. “University information assets” as used in this Article means all computer systems, applications (including email), university information and data, hardware, software, networks, internet access resources, platforms and/or devices provided by the university. University information assets are made available to bargaining unit faculty members for use in their work for the university. Any use of university information assets must comply with this Article, and applicable law, and University policy.

Section 2. Except to the extent set forth in this Agreement:

a. All university information assets belong exclusively to the University, and are not the private property of any bargaining unit faculty member.

b. The University owns all legal rights to control, transfer, or use all parts of University information assets.

c. The University may withdraw permission for use of its information assets in compliance with this Agreement, University policy, or in circumstances that pose a risk to the security or integrity of the assets or information stored on them, or a risk to the university. Except for routine withdrawals of permission (that is, when the withdrawal is the result of cessation of employment) and temporary disability of access in response to a security incident, the University shall notify the Union in a timely manner of the action taken and the reasons for the action. For temporary disablement of access in response to suspected security incidents, notice will be provided to the user of the disruption to their account within a reasonable time, generally not to exceed two weeks. Notice may be delayed until after the security threat has passed. At any time, the Union can also ask for a report of the number of accounts impacted over the last calendar year and a report will be provided within ten business days of the request. For security incidents that impact more than 100 bargaining unit members, notice of withdrawal of access will be provided to the Union within a reasonable time, generally not to exceed two weeks. Notice may be delayed until after the security threat has passed and will include an explanation of the action taken and the reason for the action.

Section 3. Bargaining unit faculty members shall not use university information assets for any unlawful purpose or in any manner that conflicts with this Agreement or University policy. Use of university information assets shall comply with copyrights, licenses, contracts, intellectual property rights, and laws associated with data, software programs, and other materials made available through those assets.

Section 4. The use of university information assets by bargaining unit faculty members shall respect the confidentiality of other users’ information. Bargaining unit faculty members shall not attempt to: (a) access third party systems without prior authorization by the system owners; (b) obtain other users’ login names or passwords; (c) attempt to defeat or breach computer or network security measures without written permission by the Provost or their designee; or (d) intercept, access, or monitor electronic files or communications of other users.

March 12, 2020
or third parties without approval from the author. Operation or use of university information assets shall be conducted in a manner that maintains the integrity of the assets and the information stored on them, and that will not impair the availability, reliability, or performance of university information assets, or unduly contribute to system or network congestion.

Section 5. Bargaining unit faculty members will use any antivirus, antimalware, or similar security related software that is furnished by the university to protect university information assets.

Section 6. Email e-mail is provided to bargaining unit faculty members primarily for university-related business; however, bargaining unit faculty members may make personal use of their university email accounts so long as that use is reasonable in amount and does not interfere with work-related duties and responsibilities or unduly contribute to hardware, software or network congestion. No use of third-party email encryption, scramblers, remailer services, or identity-stripping or identity-hiding methods is permitted except with written permission by the Office of the Provost. Notwithstanding the above, bargaining unit faculty members may use standard security features such as encryption, passcodes, or biometric access, to protect university information assets, so long as this use does not prevent the University from obtaining access to information assets to meet legal requirements. Email Email may be used for union business as set forth in this Agreement.

Section 7. Subject to law and applicable policy, authorized university personnel with a demonstrably legitimate need may access specific information assets in order to fulfill their official professional responsibilities. Limitations on this authority include the provisions of UO Policy No. IV.06.02, Data Information Asset Classification and Management Policy, requiring that such access must be only to the extent and for such time as a business need exists. The University will notify the Union in a timely manner of the action taken and the reasons for the action.

Bargaining unit faculty members will provide the University with documents, information, and data not created or stored on university information assets as required to comply with federal or state public records disclosure statutes.

Section 8. Bargaining unit faculty members may make personal use of university information assets as so long as that use is reasonable in amount, does not interfere with work-related duties and responsibilities, there is no significant cost to the university, and such use otherwise complies with this Agreement, and applicable law, and University policy.

Section 9. Bargaining unit faculty members shall not use personal hardware or software to encrypt any information owned by the university so as to deny or restrict access to the University, except in accordance with prior permission or direction from the Office of the Provost or designee. Personal devices used to access information owned by the University or for University business must comply with University policy, including any acceptable use policy, and adhere to the same security standards as University owned systems.
Notwithstanding the above, personal devices may use standard security features such as encryption, passcodes, or biometric access, to protect their devices and university information assets, so long as this use does not prevent the University from obtaining access to information assets to meet legal requirements.

Section 10. Bargaining unit faculty members shall not use university information assets for political purposes related to a candidate for public office, or a ballot measure, or for solicitations related to commercial products or services.

Section 11. A bargaining unit faculty member shall:

a. Take reasonable steps to ensure the physical security of university information assets;

b. Report missing, lost or stolen university information assets to their supervisor immediately; and

c. Take reasonable steps to prevent the release of confidential information.