f. Electronic Signature (or e-signature): A

not limited to: registering for courses, accepting financial aid awards, paying student bills, obtaining unofficial transcripts, completing electronic forms, etc.

d. Employees shall use electronic signatures to authorize all designated internal documents. Examples include, but are not limited to: submitting grades, viewing personal payroll data, accessing protected data through the administrative computing system and web applications provided by the unit, signing off on timesheets, etc.

e. Only those employees with Signature Authority delegated in accordance with SDBOR Policy 5.3 and University Policy 5:1 are authorized to execute Agreements on behalf of the University.

    i. University employees with delegated Agreement Signature Authority who execute Agreements on behalf of the University must use a secure electronic signature application that has been approved by the Vice President for Technology and Security, designee, or successor, when signing electronically. Approved and properly conforming electronic signatures are legally binding and equivalent to handwritten signatures.

    ii. University employees with delegated Agreement Signature Authority are equally accountable for properly and appropriately executing Agreements on behalf of the University whether they sign the document manually or electronically.

f. University employees who lack delegated Agreement Signature Authority, but have been designated another specified approval authority, may use an electronic signature for approving non-legal, internal documents.

g. In accordance with University Policy 5:1, the Office of the Vice President for Finance and Budget

l. It is a violation of this policy for an individual to sign a University transaction on behalf of another individual, unless they have been granted specific authority by that individual.

m. Individuals shall report any suspect or fraudulent activities related to electronic signatures immediately to the University Controller.

n. Employees who falsify electronic signatures or otherwise violate this policy and its procedures are subject to disciplinary action, up to and including termination of employment and referral for criminal prosecution under applicable federal and state laws.

o. Students who falsify electronic signatures or otherwise violate this regulation are subject to disciplinary action under the Student Conduct Code and referral for criminal prosecution under applicable federal and state laws.

p. Other members of the University community who falsify electronic signatures or otherwise violate this regulation are subject to appropriate sanctions, including but not limited to termination of the relationship and referral for criminal prosecution under applicable federal and state laws.

4. Procedures

a. Enterprise-Level Transactions:

i. The principal University administrators, data custodians, and enterprise application system owners shall assess the potential for replacing a manual process, signature, or both with an electronic process, signature, or both to automate a process and propose joint recommendations for implementation of automation, subject to approval by the Vice President for Technology and Security, designee, or successor and their Vice President. Once a process for a University transaction is approved and automated, it is automatically subject to the provisions of this policy.

b. Other transactions:

i. For all other transactions, the transaction to be enabled by e-signatures shall be evaluated by the unit, in conjunction with the Vice President for Technology and Security, designee, or successor. For risk assessment and review purposes, similar types of transactions may be grouped together under one agreement. Implemented e-

c.