THE
UNIVERSITY
OF UTAH®

To: Legislative History

From: Ken Pink, Deputy Chief Information Officer

Policy Owner(s): Deputy Chief Information Officer

Date: April 4, 2022

Re: Rule R4-050B: University Software Revision 0

Introduction and Background

Rule R4-050B: University Software provides the University the opportunity to review security and accessibility of software acquired, leased, or developed. The rule was developed following a state audit in 2018 and an internal audit in 2019 that made recommendations related to software security.

Summary of Rule R4-050B: University Software

Rule 4-050B requires, with certain exceptions, that a vendor of software that accesses, manipulates, creates, or stores restricted data, must complete the Higher Education Community Vendor Assessment Toolkit before the University purchases the software. The exceptions to this requirement include software that resides in a protected environment, software approved by the Chief Information Security Officer as an exception, and software on a machine not connected to the University network.

Regulation Development Process

University Information Technology worked with the Senate Academic Committee for Information Technology (SACIT) from 2020 through 2022, and SACIT supported the rule in February 2022. The rule was also approved by the Institutional Policy Committee. The rule was approved by the Academic Senate on April 4, 2022.

University Software Rule R4-050B Executive Summary

What does Rule R4-050B do?

- Ensures that software purchased, leased, or developed by the University is reviewed for compliance with IT security requirements
- Ensures that software purchased, leased, or developed by the University is reviewed for compliance with accessibility requirements for persons with disabilities

Why is Rule R4-050B necessary?

- 2018 State audit determined that the U was not in compliance with state security regulations
- 2019 University internal audit determined that the U was not evaluating software for risk and accessibility
- Need for appropriate multiple-office collaboration on
  - The purchase, lease, development, or other form of acquisition of University software
  - Data and services associated with requested software

What/who is covered by Rule R4-050B?

- Units in University Hospitals and Clinics
- Units in the University of Utah
- Software ***of any cost*** that is requested for purchase, lease, development, or other form of acquisition
  - ***And*** that accesses, manipulates, creates, or stores restricted data
- Note: Adherence to Rule R4-050B is recommended, but not required, for software that accesses, manipulates, creates, or stores sensitive data as outlined Rule R4-004C.

What is NOT covered by Rule R4-050B?

- Software that resides in a protected environment (PE)
  - E.g., the Center for High Performance Computing's PE, which provides HIPAA-compliant space for researchers at the University of Utah. CHPC provides hardware, software, tools, and support.
- Software approved by the CISO as an exception
- Software the does not contain restricted rata
- Software on a device that is not connected to the University network

How do U organizations comply with Rule R4-050B?

- Complete the Educause Higher Education Vendor Assessment Tool (HECVAT)
- Complete the appropriate questionnaire:
  - On Site Hosted Prospective Supplier Technical Questionnaire
  - Cloud Hosted Prospective Supplier Technical Questionnaire
- UIT will assist orgs as needed throughout this process. More info.

What closely related policies and rules are already in effect?

- University Software Policy 4-050 (2019-07-01)
- University Enterprise Software Rule R4-050A (2019-07-01)

Definitions, as per Policy 4-050

A. Software, and specific types of software, are defined as follows:

1. **Software**
   a) can be executed on a local workstation or server as well as on either a public or private cloud; and
   b) can access, delete or create public, restricted, or sensitive data as well as PHI (Protected Health Information) and HIPAA (Health Insurance Portability and Accountability Act) and University IP (Intellectual Property) data.
2. **System software** — serves as a base for application software. System software includes device drivers, operating systems (OSs), compilers, disk formatters, text editors and utilities helping the computer to operate more efficiently. It is also responsible for managing hardware components and providing basic non-task-specific functions.
3. **Programming software** — is a set of tools to aid developers in writing programs. The various tools available include compilers, linkers, debuggers, interpreters and text editors.
4. **Application software** — is intended to perform certain tasks. Examples of application software include office suites, gaming applications, database systems and educational software. Application software can be a single program or a collection of small programs. This type of software is what consumers most typically think of as "software."

B. **University Software** — is any software that is purchased, leased, or developed, or otherwise acquired by a University of Utah administrative or academic unit, for use by that University unit. It does not include software that is developed or acquired by an individual member of the University community (including any student, employee, or volunteer) without use of University funds or resources, for such individual person's private use.

C. **University Enterprise Software** — is a type of University Software defined further in University Rule 4-050A University Enterprise Software.

D. **Total Cost of Ownership (TCO) of software** — includes the costs involved for the purchase, lease, development, or other form of acquisition of software; costs for installation, and/or support of the software throughout the expected period of use by the University; and costs associated with integration of the software to other University IT systems.