Rule 4-050B University Software.

Revision #0. Effective date: April 4, 2022

I. **Purpose and Scope**

   A. Purpose.

     The purposes of this Rule include establishing a framework for identifying the scope and purpose associated with University Software (herein defined), for University of Utah Hospitals and Clinics and the University of Utah.

     The purpose of this rule is to provide the University the opportunity to review the security and accessibility of all software purchased, leased or developed by the University to ensure it meets current Information Security and Accessibility standards as determined by University Information Technology (UIT).

     The purpose of this Rule includes promoting appropriate collaboration between University administrative and academic units, including Purchasing, UIT, Risk Management, Information Security, General Counsel, Health Sciences, University of Utah Hospitals and Clinics, and University senior administration on 1) the purchase, lease, development, or other form of acquisition of University Software; 2) data and services associated with such Software, and 3) costs for the proposed software.

   B. Scope.

     This Rule applies to all units of the University of Utah Hospitals and Clinics and the University of Utah.

II. **Definitions**

   The definitions provided in Policy 4-050 apply for this rule, including the definitions of software, system software, programming software, application software, and University Software.

III. **Rule**

A. This rule applies to software that accesses, manipulates, creates or stores restricted data and is recommended for software that contains sensitive data as outlined Rule R4-004C.

B. This rule does not apply to software that resides in a University approved protected environment. The University CISO (Chief Information Security Officer) determines if the proposed environment is considered University approved.

    1. An example of a protected environment is the CHPC (Center for High Performance Computing) environment which provides a HIPAA compliant working environment for researchers at the University of Utah, referred to as the protected environment (PE). CHPC provides the hardware, software, tools and support to this user base. This is one of the currently approved protected environments. Please reach out to CHPC for specific instructions on using their environment.

C. For both University Software and University Hospital or Clinics software, if the software does not reside on equipment attached to the public internet or outside the unit it is not required to go through the security evaluation described in this rule.

D. If the software does not fall under Policy 4-050 and uses restricted data as described in Rule R-004C, before University Software is purchased, leased, developed or otherwise acquired by the University, the unit is required to complete the Educause Higher Education Community Vendor Assessment Toolkit (HECVAT) and the mandatory questions document, which must then be evaluated by UIT for campus and health sciences software. This includes University software purchased through Accounts Payable or University Purchasing as well as sole source and renewals. A failing score during the evaluation will result in the software not being approved for acquisition.

E. If University Hospital or Clinics software does not require the University Enterprise purchasing process, before it is purchased, leased, developed, or otherwise acquired by the University Hospital or Clinics, the unit is required to

complete the Educause HECVAT and the mandatory questions document, which must then be evaluated by University of Utah Hospitals and Clinics Information Technology Services (ITS). A failing score during the evaluation will result in the software not being approved for purchase.

F. If there are circumstances that require an exception to this rule, the University CIO or University Hospital CIO can make an exception to this University Software Rule.

IV—VII Regulations Resource Information.

User Note: Parts IV-VII of this Regulation (and all other University Regulations) are Regulations Resource Information – the contents of which are not approved by the Academic Senate or Board of Trustees, and are to be updated from time to time as determined appropriate by the cognizant Policy Officer and the Institutional Policy Committee, as per Policy 1-001 and Rule 1-001.

IV. Policies/ Rules, Procedures, Guidelines, Forms and other Related Resources

A. Policies/ Rules.

1. Policy 4-050 University Software Policy

B. Procedures, Guidelines, and Forms. [*reserved*]

C. Other Related Resources.

1. Technical Vendor Questionnaire

2. Three-year TCO form

3. HECVAT

V. References

A. Policy 4-004 University of Utah Information Security Policy

   B. Rule 4-004C Data Classification and Encryption

   C. G4-004D Guideline Cloud Computing: Opportunities Used Safely

VI. Contacts

The designated contact officials for this Regulation are

   A. Policy Owner (primary contact person for questions and advice): Deputy Chief Information Officer (DCIO)

   B. Policy Officer: University Chief Information Officer

See University Rule 1-001 for information about the roles and authority of policy owners and policy officers.

VII. History

Renumbering: Not applicable._

Revision History.

   A. Current version. Revision 0.

      1. Approved by -- Academic Senate April 4, 2022, with effective date of April 4, 2022.

      2. Legislative History for current version.

        Editorial Revisions: *[reserved]*