POLICY & PROCEDURE DOCUMENT

NUMBER: 5.5045

DIVISION: Information Technology

TITLE: IT Hardware, Software, or Service Acquisition Policy

DATE: February 2, 2009

REVISED: April 15, 2013; October 8, 2014; November 3, 2014; July 1, 2016; April 17, 2017

AUTHORIZED: Gordon Johnson, VP for Information Technology

I. Purpose and Scope

The purpose of this policy is to inform members of the campus community of their responsibilities regarding the purchase or acquisition of IT hardware, software, or service(s) of the type described under section **Applicable Hardware/Software/Service**. This policy defines the process and guidelines for acquiring such hardware, software, or service(s) and addresses issues resulting from non-compliance with this policy. It seeks to prevent situations where departments or administrative units purchase these items or enter into agreements that require IT resources and support to install or operate without involving IT. IT resources and support refers to programming, administration, networking, consulting, training, troubleshooting, break/fix support, server or other hardware allocation, access to central data stores, or accounts such as directory or email.

II. Policy

Acquisition Process

Any WKU employee or campus entity interested in purchasing hardware, software, or service(s) (of the type described below under **Applicable Hardware/Software/Service)** is required to contact the WKU Information Technology (IT) Division ***before*** entering into an agreement with a vendor to purchase and/or use such items either remotely or locally. IT must evaluate the purchase/use of each item to determine its resource requirements, its compatibility with other University systems and the network, its interface requirements to existing University systems if any, its security capabilities, and/or deficiencies and to determine whether a previous University system or service provides equivalent functionality.

III. Procedure

Prior to purchasing any software/hardware systems of the type described below under **Applicable Hardware/Software/Service,** do at least one of the following:

- Contact the Supply Chain Management Assistant Director. Contact information is available at http://www.wku.edu/it/vpit/staff.
- Contact IT support via one of the methods found at http://www.wku.edu/it/contact.

During the purchase of any hardware, software, or service(s) of the type described below under **Applicable Hardware/Software/Service,** do all of the following:

- If required by Supply Chain Management or IT, execute the **Contract Rider for IT Acquisitions** (attached to this policy) prior to or simultaneously to the signing of any vendor's or contractor's contract(s). Use the instructions that accompany the rider.

Applicable Hardware/Software/Service:

This policy specifically pertains to software/hardware acquisitions that fit one or more of the following criteria:

a) Any hardware, software, or service not currently supported by the IT Division but requiring IT support or resources during initial implementation or any time thereafter.
b) Hardware or software that will be installed in/on a system that is currently supported by the IT Division.
c) Software, especially multi-user software, requiring IT networking, programming, or system administration expertise to configure and operate.
d) Any system or service requiring a locally-hosted server and/or database.
e) Lab hardware or software of any type that will require configuration by and resources of the University's IT Division.
f) Systems or services that require an interface to University enterprise systems (such as Banner or Blackboard) regardless of where such systems are physically located or managed. Required interfaces to enterprise systems typically take the form of file extracts, dynamic web services, and APIs, among other types.
g) Systems or services that will store or process University data; particularly sensitive data or personally identifiable information (PII) as described in the IT Security Plan.
h) Systems or services that will process electronic payments.

Compliance/Non-Compliance.

Any member of the campus community who does not comply with and abide by this policy will not be supported by IT and may be prevented from operating or using the hardware, software, or service(s) not acquired in accordance with this policy.

Compliance with this policy does not guarantee IT support of the hardware, software, or services under consideration.

Technical Support.

Depending on the situation, IT may charge a department or unit an annual cost recovery fee for server hosting, data storage, systems administration, application programming, and/or database management services associated with operating a given software application or system. Typically, software/hardware systems that are not "enterprise-grade" and are more departmental or unit centric in nature require IT to charge cost recovery fees for support services. This is determined by IT on a case-by-case basis.

IV. Related Policies

5.501X Information Security Plan

V. Reason for Revision

Revised to add information relating to IT service purchases and to add the Contract Rider for IT Acquisitions and related language. Also added date of last review.

This policy was last reviewed on June 28, 2018.

Contract Rider for IT Acquisitions

Western Kentucky University, Revised April 17, 2017

Introduction

The document that follows is a contract rider or supplemental contract that must be attached to all IT hardware, software, and services contracts entered into between a representative of WKU and any outside party. The primary purpose of this rider is to protect data containing the personally identifiable information (PII) of all persons related to WKU. This rider must be executed prior to or simultaneously to the execution of any vendor's or contractor's contract(s) at the time of product or service acquisition. Completion of this rider is required by University policy.

Instructions

If you are a representative of WKU who is entering into a contract(s) for IT products or services with an outside party, attach this rider to any contract(s) between you and the outside party. Complete the form fields in the rider including the name and date of the agreement and name of the vendor. Upon completion of the document, forward a copy of the original contract(s) and this rider to the Assistant Director of Supply Chain Management, Western Kentucky University, 1906 College Heights Blvd, Bowling Green, KY 42101.

Contract Rider

Requirements for the Protection of University Personally Identifiable Information (PII)

Effective immediately, the following clauses in this Rider are incorporated as a part of the agreement known as _____ (herein "Agreement") between Western Kentucky University (herein "University") and _____ (herein "Vendor") dated _____ and replace or supplement the terms of the Agreement. In the event of any conflict between the terms of this Rider and the Agreement, the terms of this Rider shall govern.

1. For purposes of this Rider, Personally Identifiable Information (herein "PII") shall mean any information that, when used on its own or in combination with other information, permits the identity of an individual to be known or reasonably inferred. PII is further defined as information in any form about current or former University faculty, employees, students, prospective students, applicants, and other persons associated with University. Elements of PII include but are not limited to an individual's name, addresses, telephone numbers, email addresses, social security number, bank or other financial institution account numbers, credit or debit card numbers, driver's license number, passport number, other government-issued identification numbers, biometric data, health and medical information, education records, University ID number, employment information, gender, race, birth date, data about an individual obtained through survey or research, social media addresses or account names, "Personal Information" as described in in the Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq., and any additional categories of information about individuals that University designates in writing as Personally Identifiable Information or PII.
2. Vendor agrees that it must not share PII with, surrender PII, or provide access to PII to any third party, including but not limited to subcontractors or any other entities not affiliated with University, unless and until Vendor has been granted written approval by University.
3. Vendor agrees that it must not use or allow the use of PII for any purpose other than in the performance of services for University, and access to PII must be limited to Vendor's employees and subcontractors who have a specific need for such access in order to perform such services.
4. Vendor's employees and subcontractors must not electronically transmit PII via any means including but not limited to email, Internet, or wireless network unless the transmission is sufficiently encrypted to the definition of "Encryption" as described in the Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq.
5. Vendor's employees and subcontractors must not store PII on any portable device or media including, without limitation, laptops, PDAs, smartphones, CDs, DVDs, flash drives, external hard drives, or backup tapes unless the PII is sufficiently encrypted to the definition of "Encryption" as described in the Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq.

6. Upon termination or expiration of Agreement, or at any time upon the request of University, Vendor and its subcontractors shall return all PII (and all copies and derivative works thereof made by or for Vendor). Further, Vendor and all subcontractors shall delete or erase such PII, copies and derivative works thereof, from their computer systems.
7. To the extent that Vendor receives Personal Information as defined by and in accordance with Kentucky's Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq., (the "Act"), Vendor shall secure and protect the Personal Information by, without limitation, complying with all requirements applicable to non-affiliated third parties set forth in the Act. Vendor hereby agrees to cooperate with University in complying with the response, mitigation, correction, investigation, and notification requirements of the Act. Vendor shall notify as soon as possible, but not to exceed seventy-two (72) hours, the University of a determination of or knowledge of a breach, unless the exception set forth in KRS 61.932(2)(b)2 applies and the vendor abides by the requirements set forth in that exception. Vendor agrees to notify, in writing, the Council on Postsecondary Education in the same manner as above. The vendor hereby agrees that University may withhold payment(s) owed to the vendor for any violation of the Identity Theft Prevention Reporting Requirements. The vendor hereby agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933. Upon conclusion of an investigation of a security breach of Personal Information as required by KRS 61.933, the vendor hereby agrees to an apportionment of the costs of the notification, investigation, and mitigation of the security breach. In accordance with KRS 61.932(2)(a) the vendor shall implement, maintain, and update security and breach investigation procedures that are appropriate to the nature of the information disclosed and at least as stringent as the security and breach investigation procedures and practices of University.
8. The terms of this Rider shall survive the termination of the Agreement.

For Vendor	For University
_____	_____
Printed Name:	Printed Name:
Title:	Title: