RISK ACCEPTANCE - INFORMATION SECURITY

POLICY NUMBER: ADM-RISKACCEPTINFOSEC
POLICY TYPE: ADMINISTRATIVE
RESPONSIBLE OFFICIAL TITLE: VICE PRESIDENT OF ADMINISTRATION & FINANCE/CFO
RESPONSIBLE OFFICE: INFO. TECHNOLOGY (IT)/CHIEF INFORMATION OFFICER (CIO)
EFFECTIVE DATE: UPON PRESIDENTIAL APPROVAL – 2/8/2024
NEXT REVIEW DATE: PRESIDENTIAL APPROVAL PLUS FOUR (4) YEARS – 2/8/2028
SUPERSEDES POLICY DATED: N/A – NEW POLICY
BOARD OF REGENTS REPORTING (CHECK ONE):
☐ PRESIDENTIAL RECOMMENDATION (CONSENT AGENDA/VOTING ITEM):
☒ PRESIDENTIAL REPORT (INFORMATION ONLY)

I. POLICY STATEMENT

While it is not possible to eliminate all information security risk within an organization, Northern Kentucky University (NKU) is committed to mitigate risk to a level that is prudent.

All organizational units within NKU must take steps to reduce information security risk to a level established as best practice by the National Institute of Standards and Technology (NIST).

If an organizational unit elects not to institute a safeguard, control, or process to reduce the risk any further, and there is still a question as to whether the risk is reasonable, the associated risk or vulnerability must be clearly communicated, documented, and accepted by NKU leadership and/or their designee.

All organizational units within Northern Kentucky University are required to follow information security and university technology policies with respect to the mitigation of risk, except where there exists a strong business reason for an exemption from a particular recommendation, practice, or policy.

Unacceptable information security risk that cannot be fully mitigated in accordance with NKU's policy, standards, and procedures must be formally documented. This documentation includes submitting a Risk Acceptance Form (RAF) by the Vice President, Dean, or their designee (business owner). Before submitting the RAF, the business owner must implement and document appropriate mitigating and/or compensating controls/safeguards. These controls are intended to reduce the risk to an acceptable residual level. The IT Information Security Team must then review and approve these measures.

The IT Information Security Team is responsible for the maintenance of the RAFs as they pertain to information security. The business owner is ultimately responsible for the risk and by signing the RAF is accepting that responsibility. RAFs must be reviewed, revised, and approved on an annual basis.

II. ENTITIES AFFECTED

All Northern Kentucky University administrators, faculty, and staff

III. RESPONSIBILITIES

Information Technology (IT) Information Security Team is responsible for reviewing and tracking all requests for required risk mitigation exceptions and for reviewing and approving all exceptions on an annual basis.

IV. REFERENCES AND RELATED MATERIALS

REFERENCES & FORMS

Risk Acceptance Form

RELATED POLICIES

Vulnerability and Patch Management

REVISION HISTORY

REVISION TYPE	MONTH/YEAR APPROVED
New Policy	February 8, 2024

RISK ACCEPTANCE – INFORMATION SECURITY

PRESIDENTIAL APPROVAL

PRESIDENT

Signature Cady Short-Thompson Date 2/8/24

Cady Short-Thompson

BOARD OF REGENTS APPROVAL

BOARD OF REGENTS (IF FORWARDED BY PRESIDENT)

☐ This policy was forwarded to the Board of Regents on the ***Presidential Report (information only)***.
Date of Board of Regents meeting at which this policy was reported: _____/_____/_____.

☐ This policy was forwarded to the Board of Regents as a ***Presidential Recommendation (consent agenda/voting item)***.

- ☐ The Board of Regents approved this policy on _____/_____/_____.
  (Attach a copy of Board of Regents meeting minutes showing approval of policy.)
- ☐ The Board of Regents rejected this policy on _____/_____/_____.
  (Attach a copy of Board of Regents meeting minutes showing rejection of policy.)

SECRETARY TO THE BOARD OF REGENTS

Signature Date

Tammy Knochelmann

Risk Acceptance Form

Organizational Unit Name
Summary of Request: Safeguard, Control or Process for which Exception is Requested
Summary of Risk to NKU
Benefits of Accepting This Risk
Summary of Information Security Controls Related to This Risk
Remaining Risk After Controls:
Business Owner (Vice President or Dean, or Designee) Decision: Please choose one of the options below, and sign at the bottom of this form. The Vice President or Dean, or their designee, is required to accept responsibility for the risks associated with this exception to NKU policies and standards. □ **Yes, with Reduced Scope.** I accept responsibility for the outstanding risk related to the deployment provided. Use is reduced and limited. *List scope restraints:* □ **Yes, for Temporary Period While Controls Are Improved.** I accept responsibility for the outstanding risks related to the deployment and use of this application or service; however, I find

the current level of control inadequate. I would like to work to begin to improve controls as noted below.

List timing constraints here and/or controls requested:

□ **Unqualified Yes.** I understand and accept responsibility for the outstanding risk related to the deployment and use of this application or service for the requested scope and timeframe. I find the current controls adequate, additional controls need not be applied. *(This RAF will be reviewed and approved by the business owner and the Security Team on an annual basis).*

□ **No.** I find the residual risk greater than the potential business benefit. This risk acceptance request is denied.

I understand the risks documented in this form. I understand that compliance with university policies and standards is expected for all organizational units, information systems and communication systems and that this exception may be revoked during any phases of the executive approval process and may be subject to internal audits.

Signature of Responsible Person	Date
Printed Name of Responsible Person	

The remaining fields are for NKU Information Technology Security Team use only:

Risk Level (Low, Medium, or High):

(As determined by Risk Matrix)

Date of Next Review:

(one year from final approval, unless otherwise specified by business owner)

IT Security Team Risk Acceptance:

□ Yes, this risk can be accepted □ No, this risk cannot be accepted

Due to the potential risk and/or business impact related to this request I have deemed that this risk needs to be reviewed and approved or denied by a university executive officer. □ Yes, this risk needs further review □ No, this risk needs no further review
Signature of Chief Information Officer or Designee Date
Name Title