Risk Acceptance Form

New Mexico State University

Use this form to request risk acceptance of an identified risk associated with the use of information technology systems or services. (See the NMSU Information Technology Risk Acceptance Standard.)

Instructions:

- Requestor – Complete below through *Requesting Risk Acceptance Signatures* and sign.
- ICT Information Security Team – Review form and complete *from Level of Risk* through *CISO Approval* and sign.
- CIO and Executive Officer – Review form, complete from *CIO/Executive Office Approval* and sign.

TO BE COMPLETED BY RISK ACCEPTANCE EXEMPTION REQUESTOR

Request Date (mm/dd/yy): _____

Employee Requesting Risk Acceptance

Employee Name: _____

Employee Title: _____ Employee Department: _____

Email Address: _____ Phone No.: _____

Provide a business justification for this risk acceptance request.

By putting this solution in place, how does the university benefit?

Provide a list of NMSU data and services that are potentially at risk as a result of the known risk.

Identify data (personally identifiable/FERPA, research, financial, etc.), services, systems and/or processes impacted

What is your proposed strategy for mitigating the risk?

Also include the risk associated with proposed solution along with known vulnerabilities and possible negative outcomes.

Provide a Summary of the Security Controls that will be implemented

Describe the technical and procedural controls put in place to address the vulnerabilities and risks above. If you are not putting any controls in place simply enter *NONE*.

Provide Security Controls Documentation Details

Are security controls documented? If so, where is the documentation located?

Requesting Risk Acceptance Signature

	Date	Signature: Employee Accepting/Requesting Exemption
Name: Requestor's Director/Dept. Head (print)	Date	Signature: Requestor's Director/Dept. Head

BELOW TO BE COMPLETED BY NMSU INFORMATION SECURITY TEAM

ICT Data Security Team: Review request, complete form and submit for approval to CISO. CISO: Review and approve or forward to next level review

Level of Risk

What is the assessed level of risk with this request? --- High/Medium/Low --- Explain

Post-implementation Risk Level

Once controls are put in place, define remaining risk to the university and rank it --- High/Medium/Low

CISO Approval	
I find the risk to be as follows:	
○	**Acceptable with reduced scope**. The risk is acceptable provided the deployment scope is reduced and limited per comments below.
○	**Acceptable for a temporary period of time while controls are improved.** The current level of control is inadequate. Responsibility for outstanding risk related to the deployment and use of the above-mentioned application or service is acceptable. Improve controls, as noted below, are required along with scoping document/list, timing constraints, and controls requested.
○	**Fully Acceptable without qualification**. The risk and responsibility for the outstanding risk related to the deployment and use of this application or service for the requested scope and timeframe is acceptable. The current controls are adequate, and additional controls need not be applied.
○	**Not Acceptable.** The residual risk greater than the potential business benefit. This risk acceptance request is denied.
○	**Requires CIO approval.** Due to the potential risk and/or business impact related to this request, this risk exemption is forwarded for review and approval by University Executive officers (CIO and appropriate senior Vice President or University President).
Comments related to risk above:	

Date of Next Review: _____

_____ _____ _____

Name: Data Custodian if Applicable (print) Date Signature: Data Custodian

_____ _____ _____

Name: Chief Information Security Officer (print) Date Signature: Chief Information Security Officer

BELOW TO BE COMPLETED BY NMSU CIO/EXECUTIVE OFFICER

(Risk requiring this level of approval or that override the CISO will also be copied to the Board of Regents Audit Sub-Committee)

CIO/Executive Office Approval	
CIO - I find the risk to be as follows:	
○	**Risk is acceptable**.
○	**Approval at this level not required.**
○	**Risk is not acceptable. Fully Acceptable without qualification**.

Comments related to risk above:
_____
_____
_____
_____
_____

_____ _____ _____

Name: Chief Information Officer (print) Date Signature: Chief Information Officer

Executive Officer - I find the risk to be as follows:	
○	**Risk is acceptable**.
○	**Approval at this level not required.**
○	**Risk is not acceptable. Fully Acceptable without qualification**.
Comments related to risk above:	
_____	
_____	
_____	
_____	
_____	

_____ _____ _____

Name: Provost, Senior VP or President (print) Date Signature: Executive Officer

Appendix

Definitions

- *Acceptable risk* - A term used to describe the minimum acceptable risk that an organization is willing to take.
- *Countermeasure or safeguards* - Controls, processes, procedures, or security systems that help to mitigate potential risk.
- *Exposure* - When an asset is vulnerable to damage or losses from a threat.
- *Exposure factor* - A value calculated by determining the percentage of loss to a specific asset because of a specific threat.
- *Residual risk* - The risk that remains after security controls and security countermeasures have been implemented.

- *Risk management* - The process of reducing risk to assets by identifying and eliminating threats through the deployment of security controls and security countermeasures.
- *Risk analysis* - The process of identifying the severity of potential risks, identifying vulnerabilities, and assigning a priority to each. This may be done in preparation for the implementation of security countermeasures designed to mitigate high-priority risks.

Criticality Matrix

	Most Critical *Highest level of sensitivity*	**Critical** *Moderate level of sensitivity*	**Least Critical** *Very low, but still requiring some protection*
Legal Requirements	Protection of data is required by law (e.g., HIPAA and FERPA data elements and other personal identifying information protected by law)	The institution has a contractual obligation to protect the data (e.g., bibliographic citation data, bulk licensed software)	
Reputation Risk	High	Medium	Low
Other Institutional Risks	Information that provides access to resources, physical or virtual	Smaller subsets of Most Critical data from a school, large part of a school, or department	
Data Examples	• Medical • Student • Prospective student • Personnel • Donor or prospect • Financial • Contracts • Physical plant detail • Credit card numbers • Certain management information	• Information resources with access to Most Critical data • Research detail or results that are not Most Critical • Library transactions (e.g., catalog, circulation, acquisitions) • Financial transactions that do not include Most Critical data (e.g., telephone billing) • Very small subsets of Most Critical data	• Campus maps • Personal directory data (e.g., contact information) • E-mail • Institutionally published public data

Risk Matrix

To determine the degree of urgency attached to a given situation, refer to this table.

The Risk Matrix		**Impact**		
		High	Medium	Low
Probability	High	**A**	**B**	**C**
	Medium	**A**	**B**	**C**
	Low	**B**	**C**	**C**

Risk Assessment

The NMSU Information Security Office will assist with Risk Assessment upon request.