NMSU Information Technology Risk Acceptance Standard

V6 05 23 16

Background

Information technology (IT) is critical to the business of New Mexico State University (NMSU) and its daily operations. IT take many forms, from devices such as personal computers, smart phones, and digital assistants; to enabling technologies like the internet; to software, such as mobile phone applications and systems that run on desktops or in the cloud.

Because of the pervasiveness of technology, it is understood that its use sometimes poses risk that is not possible to eliminate. For NMSU there exists an obligation to mitigate risk to a level that allows NMSU to 1) conduct its business, 2) protect information from loss, and 3) operate in accordance with applicable laws and regulations.

As such, all NMSU organizations are required to take steps to reduce risk to a "best practices" level. When an organization elects not to reduce risk or cannot institute a control or process to reduce risk, the associated risk or vulnerability left unaddressed must be clearly communicated and accepted by the NMSU Chief Information Officer (CIO) and associated data custodians or their designee.

Standard

In regards to mitigation of risk, all NMSU organizations are required to follow the best practices for their respective industries except where there exists a strong business reason to exempt an organization from a particular industry best practice.

For risk exceptions, the following applies:

- A legitimate business reason/case for risk exception must be present;
- All risk exceptions must be documented and approved by senior management;
- Risk exception approvals will be granted or denied via the completion of the Risk Acceptance Form (RAF) (See Related Forms/materials section of this policy.);
- A RAF must be initially signed by a manager and then forwarded to the Chief Information Security Officer (CISO) for review and approval or denial or escalation to more senior management;
- The CISO is responsible for the maintenance of the Risk Acceptance Form.

Scope

This standard applies to all NMSU organizations.

Standard Administration

This standard is administered and maintained by the NMSU CIO.

Definitions

- *Best Practice:* A concept which asserts that there is a technique, method, process, or activity that is more effective at delivering a particular outcome than any other. Descriptions of best practices are normally available from a variety of sources including affinity groups, professional associations, and certifying or regulating authorities for an industry.
- *Information Technology:* technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data.
- *Risk:* A concept that denotes a potential negative impact or something that increases the probability of a loss.
- *Risk mitigation*: Actions taken to reduce the probability that the loss represented by the risk will occur. Mitigation recognizes that the purpose of an organization is to deliver services and goods to their respective customers to meet business goals. It provides for cost/benefit analysis of a mitigating action prior to implementation.

Applicable Laws and Guidelines

NMSU must adhere to laws and guidelines as part of its normal business activities. These include the following:

- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry Data Security Standards (PCI DSS)
- Red Flag Rule
- Application of Best Practices for managing information security such as those offered by Control Objectives for Information and related Technology (COBIT), relevant International Organization for Standardization (ISO) standards, National Institute of Standards and Technology (NIST), EDUCAUSE and resources offered by national and international professional associations.

Disciplinary Actions

Violation of this standard may result in any of the following:

- Revocation of network access for affected system(s)
- A recommendation of disciplinary action in accordance with NMSU HR policies
- A recommendation cessation of business relations in the case of contractors or consultants
- A recommendation of dismissal for interns and volunteers from university programs and business operations

Related Forms/materials

Risk Acceptance form – Available by email at CISO@nmsu.edu or for download from ICT.nmsu.edu/guidelines.