PURPOSE

The purpose of this standard is to document the process for requesting and reviewing exceptions to security policies and standards.

SCOPE

This standard applies to all requests for exceptions from published Information Security policies and standards.

STANDARD

Each request for an exception will be reviewed by the Information Security Officer. Where appropriate the Information Security Officer will convene an ad hoc committee to assist in evaluating the requested exception.

The Information Security Officer may invite any technical experts, including “domain experts” from other groups to participate in meetings and discussions. Their input will be considered, and they may be able to provide auxiliary determinations of feasibility or commitments of resources.

Documentation

A log of exception requests and their dispositions shall be maintained by the Information Security Officer. For each request, the log shall maintain at least the following information:

1. Requester contact information: Name and phone number.
2. The policy or standard from which an exception is requested.
3. A brief description of the justification for the request, including the organizations that would benefit from the exception.
4. A technical description of the situation that is to exist after grant of the exception.
5. A risk analysis, including the organizations that might be put at risk by the exception.
6. The organizations responsible for implementing the exception.
7. The date the request was reviewed.
8. The disposition of the request: denied, granted, granted with modifications.
9. The expiration or revisit date of granted exceptions.
10. The names of the experts or contributing reviewers.
11. Notification of the requestor.

DEFINITIONS

None.

RESPONSIBILITIES

Confidential
Information Security Exception Requesters are responsible for providing the required documentation in support of their requests. The Information Security Officer is not responsible for developing technical analyses of requests. If such analyses are not forthcoming, the associated request may be denied.

ADMINISTRATION AND INTERPRETATIONS

This standard shall be administered by Information Security. Questions regarding this policy should be directed to the Information Security Officer.

AMENDMENT/TERMINATION OF THIS POLICY

The University reserves the right to modify, amend or terminate this standard at any time. This standard does not constitute a contract between the University and its faculty or employees.

REFERENCES TO APPLICABLE STANDARDS

- Information Security Philosophy
- Information Security Governance Policy
- Information Security Exception Policy
- Information Security Exception Form

EXCEPTIONS

None.

VIOLATIONS/ENFORCEMENT

None.