



Security Exception Reporting Process

Effective Date: March 16, 2007

[Purpose](#)

[Scope](#)

[Description](#)

[Process](#)

I. Purpose

This reporting process serves as a supplement to *The Information Resources Security Operations Manual*, The University of Texas at Dallas' implementation of UT-System *UTS 165*. Adherence to the process will increase the security of systems and help safeguard university information technology resources.

It is the intent of the Information Security Office (ISO) that all owners and custodians of information technology resources adopt The University Information Resources security policies and procedures. However, there will be situations where the strict application of a policy would significantly impair the functionality of a service and the policy or procedure must be modified to accommodate specific requirements. This process provides a method for documenting an exception to compliance with a published university security policy or procedure.

II. Scope

This process applies to all published university information security standards and procedures. This process does not apply to specific department standards or procedures.



III. Description

An exception to a published policy or procedure may be granted in any of the following situations:

- Temporary exception, where immediate compliance would disrupt critical operations.
- Another acceptable solution with equivalent protection is available.
- A superior solution is available. An exception will be granted until the solution can be reviewed, and standards or procedures can be updated to allow the better solution.
- A legacy system is being retired (utilize a process to manage risk).
- Lack of resources.

IV. Process

The Information Resources owner must acknowledge and approve all requests for exceptions to university policy. The Information Security Office is available for assistance at all stages of this process.

After acknowledging and approving an exception is needed, the Information Resources owner or their designee must submit an Exception Request form to the Information Security Office (See Exception Request form).

The Security Exception Request must include:

- System(s) associated (for example, host names or IP addresses).
- Data Classification Category(s) of associated system(s).
- Description of the non-compliance.
- Anticipated length of non-compliance.
- Assessment of risk associated with non-compliance.



**THE UNIVERSITY OF TEXAS AT DALLAS
INFORMATION SECURITY**

- Plan for alternate means of risk management.
- Metrics to evaluate success of risk management (if risk is significant).
- Review date to evaluate progress toward compliance.

The Information Security Office will report exceptions to university Internal Audit and Compliance officials, as required by *UTS 165*.

[Exception Request Form](#)