

# Security Exception Reporting

---

1. Purpose .....	1
2. Scope.....	1
3. Description .....	1
4. Process .....	2
5. Revision History .....	2
6. Approvals .....	2

## 1. Purpose

This reporting process serves as a supplement to [Information Resources Use and Security Policy](#), The University of Texas at Austin’s 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 university IT 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.

## 2. Scope

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

## 3. 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).

## Security Exception Reporting

Document Version: Approved

- Lack of resources.

## 4. Process

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

After approving an exception, the IT owner or their designee must submit an Exception Request to the Information Security Office using the [online Security Exception Request Form](#).

The Security Exception Request must include:

- Description of the non-compliance
- Anticipated length of non-compliance
- Assessment of risk associated with non-compliance
- System(s) associated (for example, host names or IP addresses)
- Data Classification Category(s) of associated system(s)
- 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 may report exceptions to university Information Security Policies to university compliance officials, as described in the [Information Resources Use and Security Policy](#).

## 5. Revision History

Version	Date	New	Original
<b>Security Exception Reporting Process.docx</b>	2/3/2011	Converted web page to PDF	No change
<b>(online)</b>	10/1/2009	Updated visual appearance to new template. Corrected any out of date links to ensure they are pointing to the most current policy documents.	
<b>(online)</b>	9/14/2007	Replaced reference to BPM 53 with UTS-165.	"BPM 53"

## 6. Approvals

Name	Role	Members	Date
<b>Chief Information Security Officer</b>	Approval	Cam Beasley	1/1/2006