

INFORMATION SECURITY EXCEPTION PROCESS

1.0 Purpose

This process provides a method of obtaining an exception to compliance with a published security standard or procedure.

2.0 Scope

This process applies to all published information security standards and procedures. This process does not apply to standards or procedures published by groups outside of the Information Security Office.

3.0 Description

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

- Accidental non-compliance (unaware of the published standard or procedure).
- Another acceptable solution is available (with equivalent or better protection).
- A better solution is available (an exception will be granted until the standard or procedure can be updated to include the better solution).
- A legacy system is being allowed to die (a risk managed death).
- Lack of resources (risk needs to be managed)

4.0 Process

The Information Trustee (Dean or VP) must submit the Exception Request Form to the Information Security Officer, infosec@rit.edu, Eastman Bldg, Rm. 3300.

If the non-compliance is due to anything other than a superior solution, the Exception Request must include:

- Description of the non-compliance
- Anticipated length of non-compliance
- Assessment of risk associated with non-compliance
- 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.

If the non-compliance is due to a superior solution, an exception will automatically be granted until the published standard or procedure can be revised to include the new solution.

5.0 Exception Process Form

To download the form, go to

http://security.rit.edu/process/Exception_request.doc.