INFORMATION SECURITY EXCEPTION PROCESS
(Revised 7/24/12)

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 MAY be granted by the RIT Information Security Office for non-compliance with a standard resulting from:

- Implementation of a solution with equivalent protection.
- Implementation of a solution with superior protection.
- Impending retirement of a legacy system.
- Inability to implement the standard due to some limitation

Exceptions are granted for a specific period of time, not to exceed one year. Exceptions are reviewed on a case-by-case basis and their approval is not automatic.

4.0 Process

The Exception Request Form must be submitted to the Information Security Office, infosec@rit.edu, Ross Building 10-A200.

The Exception Request must include:

- Description of the non-compliance
- Anticipated length of non-compliance (2-year maximum)
- Proposed assessment of risk associated with non-compliance
- Proposed plan for managing the risk associated with non-compliance
- Proposed metrics for evaluating the success of risk management (if risk is significant)
- Proposed review date to evaluate progress toward compliance
- Endorsement of the request by the appropriate Information Trustee (VP or Dean). NOTE that this endorsement may be provided by email.

If the non-compliance is due to a superior solution, an exception will normally be granted until the published standard or procedure can be revised to include the new solution. An exception request must still be submitted.

5.0 Exception Process Form

To download the form, go to https://www.rit.edu/security/content/exception-process.