Information Technology Security Exception Process

Information Technology Security Procedure #3, v2.0

Standards Name: IT Security Exception Process

Original Release Date: 5/17/2006
Latest Revision Date: 10/22/2007

Authority: This procedure was approved by the Information Security Council, acting as representatives of the CIO and the Technology Leadership Committee (TLC). It derives its authority from the CIO and the campus Information Technology (IT) community.

Summary: This procedure defines how units and Users may request an exception to an IT Security Standard. Unless more specific exception methods are indicated in a standard, it applies to all IT Security Standards.

Applicability/Scope: Applies to all campus users.

Responsible Office: ITS/CIO.

Overview

Individuals and units using the University network and IT resources are expected to follow the IT Security Policies and Procedures. However, there will be cases where compliance with these Policies and Procedures cannot be achieved, for a variety of reasons. This document defines the cases in which non-compliance may be allowed (by requesting an exception) and details the exception process. The exception process usually involves the requestor, the Information Security Council (ISC) and the Information Security Officer (ISO), with the ultimate arbiter of any disputes being the CIO.

For the exception process to be effective, it must operate in a consistent, neutral and timely fashion. If a certain type of exception is constantly being requested or approved, it may mean the relevant standard needs to be adjusted to include the exception as a norm. The ISC will review these patterns and recommend changes as needed.

Note that the Exception Process is intended to be a generic method that applies to all IT Security Policies and Procedures and that the enforcement procedures for devices not in compliance are defined in those Policies and Procedures.

Conditions for Considering an Exception

- User or Unit was unaware of their non-compliance and cannot meet compliance immediately

- Insufficient resources for reaching compliance; options include acceptance of the risk, deferring the risk (insurance), or managing the risk in a well-understood manner
- Compliance is not possible and system is being phased out; the operator must manage the risk in the interim
- An alternate method for meeting compliance is available that offers equivalent or better security

Exception Process

1. The Unit IT Leader or the individual must submit the following to itsecurity@listserv.syr.edu:
2. A general description of the Exception Request, including:
    a) Description of why they are not in compliance
    b) Risks posed by non-compliance
    c) Methods and resources to be used to either meet compliance or manage the risk
    d) Date by which compliance will be met or state of non-compliance ends
3. The ISO will perform an initial analysis of the request. If the non-compliance is due to the requestor using an alternative and superior solution or if the request is clearly reasonable and fits prior patterns of approval, the ISO may automatically grant the exception. This is likely to cover 90% of all requests.

    Methods of compliance that might lead to improvements in existing Policies and Procedures may be submitted to the ISC for review and future inclusion.

4. Otherwise, the request will be presented to the ISC, within 1 business day of the request, and they will reach a decision within 1 week of receiving the information.
5. If the request is denied, it will be accompanied by an explanation and perhaps suggestions for alternative methods.
6. The result will be returned to the requestor, who may appeal denials by resubmitting the request. Appeals will be taken to the CIO, who will make the final ruling.
7. A log of exception requests and rulings will be maintained and made available to ITS management and Unit IT Leaders as needed.
8. Once a particular type of exception has been ruled on, future exception requests of the same type will receive the same ruling, barring special circumstances.

Related Policies

IT Security Standards:

- The Information Security Standard defines the classes of University Data and the protections that must be applied to them.
- The Remote Access Standard defines methods and procedures for remotely accessing University Data or transporting University Data.
- The Server Security Standard covers all devices functioning as a server.
- The Desktop Security Standard covers all PC's and laptops functioning as end user devices.
- The Authentication (password) Standard covers all systems that use user authentication.

Example

The campus currently blocks inbound ftp connections from the Internet. A researcher needs to offer anonymous ftp to fellow researchers on the Internet, so they can download various documents. The researcher has locked down the ftp service so that it is read-only (no uploading) and runs on a dedicated and secured server that contains no sensitive data. Since there is little risk to the server or the campus by granting this exception, the ISO would run some verification scans and approve the exception. The turnaround for such a case would be about one business day.