

The Information Security Policy and the standards and procedures issued by the Information Security Office institute controls for protecting University information assets. While every exception to a policy weakens protection for the underlying information, occasionally exceptions will be needed. This procedure defines the process for the review and approval of exceptions to information security standards and procedures where the cost to remediate academic or administrative practices and systems not compliant with the Information Security Policy, standards and procedures greatly exceeds the risks.

1. A manager seeking an exception (or the manager's designee) must assess the risks of non-compliance to *university resources* and business processes. The assessment must include:
 - Identification of the threats and vulnerabilities
 - How likely each is to occur and the potential costs of an occurrence
 - Cost of compliance
2. If the manager believes the risk is reasonable because compliance would (a) materially adversely affect the accomplishment of academic or administrative objectives, (b) cause a major adverse financial impact that would not be offset by the reduced risk occasioned by compliance, and/or (c) adversely reflect upon the University's reputation, and is willing to accept responsibility for the risk, then the manager must submit a completed Information Security Exception Form and supporting documentation to the University Information Security Officer. The request must include:
 - Valid academic or administrative justification
 - Risk analysis
 - Compensating controls to manage risk
 - Technical reasons for the exception
3. The University Information Security Officer will consult with University Information Technology Services, the University of Arizona Information Security Advisory Committee (UA-ISAC), Data Stewards, departmental computing managers and/or Internal Audit to the extent necessary.
4. The University Information Security Officer, or a designee, will approve or deny the request for an exception. Requests are viewed for validity and are not automatically approved. Requests that create significant risks without compensating controls will not be approved.

5. The Information Security Office will notify the requesting manager of the decision to approve or deny the request for an exception.

6. Exceptions are valid for a one-year period. Annually, the Information Security Office will send a copy of approved exceptions to the requesting manager, who must determine whether the assumptions and conditions that justified the original exceptions have not changed. If the conditions have substantially changed, a new request for exception must be submitted. If the conditions have not substantially changed, the requesting manager should make necessary updates and resubmit the request for exception to the University Information Security Officer. Where little has changed, the review process may be shortened as recommended by the University Information Security Officer, or his or her designee.

Related Guidance

Information Security Policy (IS0100) and all related standards and procedures
Information Security Terms Guideline (IS-G100)

Revision History

Initial Draft	08/28/08
Effective Date	08/28/08