# Standard Enforcement Exception Request Procedure

1. **Document Classification**
2. **Purpose**
3. **Initiation**
4. **Requesting an Exception**
   - 4.1 Requesting an extension
   - 4.2 Requesting a waiver
   - 4.3 Appealing a previous extension/waiver decision
   - 4.4 Appealing the terms of the standard
5. **Resolution**
6. **Procedure Review and Revision**

---

Version 1.0
Spring 2010
1 DOCUMENT CLASSIFICATION
This document is classified University Public. The document may be shared internally and/or externally and is published online at http://getprotected.asu.edu.

2 PURPOSE
ASU has published standards to protect University network and information systems from compromise and ensure University compliance with applicable laws, rules, and regulations. The Information Security Office will take actions necessary and appropriate to ensure compliance with those standards.

On identification of a security incident or a violation of published standards, the Information Security Office will notify responsible parties of the matter and the acceptable timeframe for resolution. If special circumstances render timely compliance impossible, or if the standard is deemed inappropriate, exceptions will be considered on a case-by-case basis. This document describes the procedure for requesting an exception.

3 INITIATION
The Information Security Office notifies responsible parties using the University's standard case resolution mechanism, PeopleSoft CRM. On identification of a security incident or a violation of published standards, the Information Security Office will create a CRM case including details of the situation and assign it to the responsible party or to a third party responsible for making case assignments (e.g., the TAG Security provider group).

4 REQUESTING AN EXCEPTION
Three forms of exception requests are possible:

- **Extension**: If the responsible party intends to comply, but cannot do so within the specified timeframe.
- **Waiver**: If the responsible party does not intend to comply because of mitigating circumstances.
- **Appeal**: If the responsible party wishes to request re-evaluation of an earlier extension or waiver request, or to express concerns regarding the requirements of the standard.

4.1 Requesting an extension

1. Notify the appropriate departmental authorities and sponsors of the risks of continued non-compliance; e.g., cost of recovery if a vulnerability is exploited, or liability if High Risk or Confidential information is exposed.

2. Add a note to the CRM case. The note should include at least the following information:
   - A complete explanation as to why timely compliance is not possible
   - Details of any compensating controls applied
   - The specific target date requested
   - Contact information in the event further information is required
   - Confirmation that the appropriate departmental authorities and sponsors understand and accept the risks of continued non-compliance

3. Re-assign the case to the Information Security Requests provider group (UTOSECISUE). The case should be kept open and assigned as a request.
4.2 Requesting a waiver

1. Notify the appropriate departmental authorities and sponsors of the risks of continued non-compliance; e.g., cost of recovery if a vulnerability is exploited, or liability if High Risk or Confidential information is exposed.

2. Add a note to the CRM case. The note should include at least the following information:
   - A complete explanation as to why compliance is not possible or desirable
   - Details of any compensating controls applied
   - Contact information in the event further information is required
   - Confirmation that the appropriate departmental authorities and sponsors understand and accept the risks of continued non-compliance

3. Re-assign the case to the Information Security Requests provider group (UTOSECISUE). The case should be kept open and assigned as a request.

4.3 Appealing a previous extension/waiver decision

Appeals of previous extension/waiver decisions should be made using the same procedures described above. Appeals will not be considered in the absence of significant new information that might affect the executive decision.

4.4 Appealing the terms of the standard

Any standard may be appealed using the Revision Request Form that appears in the body of the standard. On completion, the form should be submitted to the Information Security Office by electronic mail to infosec@asu.edu or by other mechanisms identified on the form.

Submission of an appeal does not negate responsibility for timely compliance. An extension or waiver request should be submitted if the responsible parties anticipate difficulty meeting the compliance requirements of a specific case.

5 RESOLUTION

The Information Security Requests provider group will present submitted exception requests to the Information Security Officer, who will consider requests on a case-by-case basis. The Information Security Officer will collaborate with the University Executive Team as necessary and appropriate to review exception requests.

Appeals of previous decisions will be considered only if circumstances have changed significantly or new information is available that might affect an executive decision. The Information Security Officer will review such appeals in collaboration with the University Executive Team.

 Appeals of the terms of a standard may be reviewed either during the document's annual review/revision period or during an interim review process, at the Information Security Officer's discretion, in consideration of the urgency and/or case-specific nature of the matter.

6 PROCEDURE REVIEW AND REVISION

Procedures are subject to review and revision by the Information Security Office as necessary. This procedure was last reviewed and revised in June 2010. This version was approved in June 2010 by the Information Security Officer and supersedes all previous versions, effective immediately on publication.