

| | | | |
|--|----------------------------|----------------------|------------|
|  California DEPARTMENT OF TECHNOLOGY | | 3502 | |
| INFORMATION SECURITY EXCEPTION REQUEST PROCEDURE | | | |
| OWNER: | Security Management Branch | ISSUE DATE: | 5/12/2008 |
| DISTRIBUTION: | All Employees | REVISED DATE: | 12/31/2015 |

This document was last reviewed/updated in December, 2015.

SECTION 1 – INTRODUCTION

The Security Management Branch (SMB) publishes information security policies and multiple supporting security standards and procedures to ensure a safe and secure working environment for its customers, visitors, and employees. These security policies and procedures are written to directly reflect the position of the California Department of Technology (CDT), Information Security Office; they should be adhered to by customers, visitors, and employees. The SMB is aware that exceptions can occur from time to time. This document explains the exception request procedure for a SMB policy or procedure.

SECTION 2 – EXCEPTION REQUEST PROCEDURE

Exception Qualification

The exception request procedure should be followed if either of the criteria below applies.

1. The security policy or procedure in question cannot be adhered to for unforeseen reasons outside of your control.
2. In working closely with the SMB, alternative solutions have been exhausted and are not possible.

Exception Request Procedure

Information security policy or procedure exception requests must be linked to an existing Service Request. The following procedure begins when a customer or employee has an exception request to a published security policy or procedure:

1. A SMB representative provides risk assessment and alternative recommendations to the requester's Information Security Officer (ISO); doing so may involve more CDT subject matter experts.
2. The requester's ISO either accepts or declines the assessment and alternative recommendations.
 - a. If the requester's ISO accepts, the SMB works with the customer to re-architect the issue to mitigate security risk(s). The exception is terminated and efforts continue.

- b. If the requester's ISO declines, the requester must complete the Security Policy/Standard Exception Request Form, TECH 358. The SMB manages the form and will place a reference in the corresponding Service Request.
3. The SMB will conduct meetings with the ISO to discuss the request background, documentation, risk assessment and recommended alternative.
4. The CDT ISO either accepts or declines the exception request.
 - a. If the CDT ISO accepts the request, SMB staff document responses from the requester and CDT ISO. SMB will send copies of the findings to the requester's ISO. The exception request is approved, the exception is implemented.
 - b. If the CDT ISO declines the request, SMB staff drafts and sends a formal exception denial letter to the requester's ISO. SMB staff continues to work with the requester until an acceptable solution can be agreed upon. The exception terminates, and documentation is filed and noted in the Service Request.

SECTION 3 – APPLICABILITY AND EXCLUSIONS

- A. This Procedure applies to customers and employees. Direct any questions regarding the applicability of this Procedure to the SMB for clarification.
- B. Exceptions will be considered on a case-by-case basis. Requests for an exception to a security policy or procedure must be submitted to the SMB via the Security Policy/Standard Exception Request Form, TECH 358.

SECTION 4 – AUDITING AND REPORTING

- A. Information security exception requests must be tied to a Service Request for tracking.
- B. Auditing may be performed on a periodic or random basis by the SMB or its designees. In the event an audit determines this Procedure is not being applied, notification will be sent to the appropriate person for remediation.
- C. Any known violations of this Procedure must be reported to the CDT ISO and the reporting employee's immediate supervisor.

SECTION 5 – AUTHORITY/REFERENCES

[Security Policy/Standard Exception Request Form, TECH 358](#)

Please contact your OTech Customer Representative for the document below:
3500 – Security Awareness Policy