

 California DEPARTMENT OF TECHNOLOGY		3121	
FIREWALL AND ACCESS LIST REQUEST PROCEDURE			
OWNER:	Security Management Branch	ISSUE DATE:	2/6/2008
DISTRIBUTION:	Office of Technology Services Employees	REVISED DATE:	12/31/2015

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

SECTION 1 – INTRODUCTION

The Office of Technology Services (OTech) utilizes firewalls and access lists to maintain the confidentiality, integrity, and availability of the network. A firewall is any device that directs or controls traffic between lower trust networks and higher trust networks. They secure a network by shielding it from access by unauthorized users. In an effort to maintain the highest level of firewall security, it is important that OTech staff and customers follow this procedure when requesting firewall configuration additions, changes, or removals.

SECTION 2 – STANDARD REQUIREMENTS AND REQUEST PROCEDURE

Standard Requirements

OTech firewall configurations must:

- A. Be configured based on the Principle of Least Privilege and traffic is denied unless explicitly permitted. The goal of Least Privilege is to give users only the access and privileges they need to complete the task at hand.
- B. Undergo periodic assessments to ensure the integrity of the configuration.
- C. Only be performed on approved formal request via the procedure below.
- D. Only open required ports. Requests to “open all ports” will be denied.

Request Procedure

Listed below is the firewall and access list request procedure for OTech firewall configurations.

1. A Firewall and Access List Request Form, OTECH 363, must be submitted via the Customer Service System (CSS). Only the owner of the data traffic that will be passing through the firewall or the data owner’s OTech Customer Account Representative are permitted to submit these requests.
2. Firewall or access list requests must be tied to a Service Request that either initiates a project or has costs associated with it. The initiating Service Request number must be referenced on the succeeding request.

3. The CSS request must be routed to the customer Information Security Officer (ISO) for approval **prior** to being routed to the California Department of Technology (CDT) ISO for approval. Requests not approved by the customer ISO, will not be approved by CDT. Listed below is a sample routing pattern for these requests:
 - a. OTech Customer Account Representative or data owner (requestor)
 - b. Customer determined staff (approvers may vary by request)
 - c. Customer ISO (approver)
 - d. CDT ISO (approver)
 - e. OTech Network Engineering (configuration implementers)
 - f. Should the customer ISO not have access to the CSS, an email stating their approval of the request is permitted as long as that email is attached to the request for the CDT ISO's acknowledgment.
 - g. Once the required approvers have authorized the request, it will be sent to the OTech Network Engineering staff for implementation of the configuration(s) via a Remedy Change Request. The Firewall or Access List Service Request number must be referenced in the Change Request.
 - h. No OTech Remedy Change Request is permitted to be initiated without the prior completion of the above five steps.

SECTION 3 – APPLICABILITY AND EXCLUSIONS

- A. This procedure applies to applicable OTech firewall and access list resources and anyone accessing or supporting them. Direct any questions regarding the applicability of this procedure to the Security Management Branch for clarification.
- B. Exceptions to this procedure must be documented and will be considered on a case-by-case basis. Requests for an exception to this Procedure must be submitted via the Security Policy/Standard Exception Request Form, TECH 358.

SECTION 4 – AUDITING AND REPORTING

- A. Auditing may be performed on a periodic or random basis by the Security Management Branch 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.
- B. Any known violations of this procedure must be reported to the CDT Chief Information Security Officer and the reporting employee's immediate supervisor.

SECTION 5 – AUTHORITY/REFERENCES

[Firewall and Access List Request Form, OTECH 363](#)
[Security Policy/Standard Exception Request Form, TECH 358](#)

Please contact your OTech Customer Representative for the below document:
3100 – Asset Protection Policy