



HOSTED PROJECT SECURITY STANDARD AND RECOMMENDATIONS

OWNER:	Security Management Branch	ISSUE DATE:	5/29/2008
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) has developed high level security requirements and recommendations for systems hosted at the Office of Technology Services (OTech). This Standard applies to hosted environments that process, transmit, and/or store confidential, sensitive, or personally identifiable data.

SECTION 2 – STANDARD REQUIREMENTS

Part I - Hosted Project Security Requirements

Listed below are the security requirements for any project containing public facing applications:

1. Network Architectures: The Security Management Branch approves the below two network architectures. Please refer to 3117 - Network Architecture Standard for detailed information.

Firewall with Public-Facing Web Service Ports Open	Public Facing DMZ Tier	Firewall with Application Ports Open	Application Tier	Firewall with Database Ports Open	Data Tier
--	-------------------------------	--------------------------------------	-------------------------	-----------------------------------	------------------

Firewall with Public-Facing Web Service Ports Open	Public Facing DMZ (Proxy) Tier	Firewall Application Ports Open	DMZ & Application & Data Tier ONLY for z/OS Tier
--	---------------------------------------	---------------------------------	---

2. Isolated virtual local area networks (VLANs) must exist per customer; it is desirable that each customer project be implemented in its own VLAN. Due to performance concerns of OTech firewalls, however, isolated VLANs per customer are appropriate.
3. Data repositories containing confidential, sensitive, or personally identifiable information must reside on a firewalled VLAN separate from the DeMilitarized Zone (DMZ) & application tier(s).

4. Provide detailed network architecture diagrams and data flow diagrams, including ports, protocols, and hardware placement, prior to procurement or implementation of any device. This documentation should be provided to your OTech customer account representative and/or project manager, the earlier the better, so that security concerns can be brought to light mitigating any delay to the project schedule. The account manager and/or project manager will provide the documents to the appropriate OTech project resources.
5. No database management systems are allowed on a public Internet accessible network.
6. Web services may not be installed on database or data repository servers. Web services may be installed on application servers if communication traverses either a proxy server or web server in the public facing DMZ first.
7. Authentication devices cannot reside in the DMZ; e.g., Domain Controllers and Active Directories.
8. Systems that require outbound email notifications must utilize the OTech Simple Mail Transport Protocol (SMTP) relay service.
9. Systems must adhere to OTech security and system configuration requirements, which includes but is not limited to 3126 - Server Security Standard and 3128 - Server Virtualization Security Standard.
10. Systems that process, store, and/or transmit payment card data must adhere to current Payment Card Industry (PCI) standards. The customer or vendor responsible for building and/or designing the system must provide OTech with documentation of the system's PCI compliance prior to implementation.
11. Firewall ports are closed by default for testing, development or production environments. Requests for "all firewall ports to be opened" will be denied. Request specific ports or a range of ports as early as possible.
12. Firewall port and access control list request changes should be made via a service request with the Firewall and Access List Request Form, OTECH 363, attached. Please refer to 3121 - Firewall and Access List Request Procedure for detailed information.
13. Approval by the information security officer (ISO) of the **data owner** is required, prior to implementation on all service and change requests involving:
 - Consulting for security or operational recovery.
 - Confidential or sensitive data.
 - Dial-in lines.
 - Non-state users accessing the system/data.
 - Firewall port or access list requests.
14. System data must be classified by the customer per the State Administrative Manual (SAM) section 5320.5 and disclosed to your OTech customer representative or project manager. Customer managed services, also known as SB 954, and hosted systems containing unclassified data will adopt the most restrictive security measures by default. These security measures may

result in additional costs to the customer. Refer to 3113 - Data Classification Standard for further details.

15. Confidential, sensitive, and personally identifiable information must be encrypted in transit and at rest while in publicly accessible DMZs. Encryption must adhere to the Federal Information Processing Standard Publications (FIPS) 140-2.
16. Campus to Campus communications (excluding the OC192 circuit), where confidential, sensitive, or personally identifiable information is processed, must be encrypted in transit.
17. No direct public access to the application and database tiers is permitted.
18. Publicly accessible front-end servers (web or web/application) may never have mapped network drives to back-end database servers.
19. Customer virtual private network (VPN) accounts to the hosted environment may not be shared. If the VPN account is requested for the customer's *vendor* to access the hosted environment, the customer ISO must approve the service request. Hosted environments must subscribe to the OTech VPN service; a third party VPN connection may not be established.
20. Foreign (non-OTech managed) devices are not permitted within the following OTech services:
 - Application Hosting
 - Storage
 - CA. Mail
 - Server Based Computing
 - Network
 - Recovery
 - OTech internal local area network

Part II - Hosted Project Security Recommendations

Listed below are recommendations for hosted projects:

1. Confidential, sensitive, and personally identifiable information should be encrypted while traversing the public Internet. Encryption should adhere to the Federal Information Processing Standard Publications (FIPS) 140-2.
2. Provide notice to OTech *prior* to application patching and/or maintenance so that technicians are aware and do not take unnecessary actions. This applies to all system environments; e.g., test, development, training, pre-production, or production.

Part III – Office of Technology Services Security "Facts"

Listed below are routine OTech security activities affecting hosted projects:

1. Intrusion Prevention Systems (IPS) is active at the OTech perimeter. IPSs are not host based.

2. Vulnerability scans of production servers take place regularly. Reports can be shared with customers upon request. A one-hour consulting rate fee per month will be charged for this service.

Part IV - Glossary

Listed below is the Security Management Branch’s interpretation of some information technology terms and/or concepts:

Common Term/Concept	SMB Term/Concept
Internet/public facing tier	Demilitarized Zone (DMZ)
World Wide Web	Public Facing
<i>n</i> -tiered architecture tiers or layers	Tiers
Inter-Agency Internet or Intranet	CGEN

SECTION 3 – APPLICABILITY AND EXCLUSIONS

- A. Intranet web service applications, via California Government Enterprise Network (CGEN), are not held to the above architectural requirements.
- B. This Standard does not apply to systems in the Tenant Managed Services environment.
- C. Exceptions to this Standard must be documented and will be considered on a case-by-case basis. Requests for an exception to this Standard must be submitted via the Security Policy/Standard Exception Request Form, TECH 358. Please refer to 3502 – Information Security Exception Request Procedure for detailed information. Direct any questions regarding the applicability of this Standard to the Security Management Branch.

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 Standard is not being applied, notification will be sent to the appropriate person for remediation.
- B. Any known violations of this Standard must be reported to the California Department of Technology Chief Information Security Officer and the reporting employee’s immediate supervisor.

SECTION 5 – AUTHORITY/REFERENCES

[Federal Information Processing Standard Publications \(FIPS\) 140-2](#)
[State Administrative Manual \(SAM\) section 5320.5](#)
[3113 – Data Classification Standard](#)
[3117 – Network Architecture Standard](#)
[3121 – Firewall and Access List Request Procedure](#)
[Security Policy/Standard Exception Request Form, TECH 358](#)
[Firewall and Access List Request Form, OTECH 363](#)

Please contact your OTech Customer Representative for the below documents:

3100 – Asset Protection Policy

3126 – Server Security Standard

3128 – Server Virtualization Security Standard

3502 – Information Security Exception Request Procedure