

 California DEPARTMENT OF TECHNOLOGY		3111	
TENANT MANAGED SERVICES SECURITY STANDARD			
OWNER:	Security Management Branch	ISSUE DATE:	6/6/2007
DISTRIBUTION:	Office of Technology Services Employees	REVISED DATE:	12/31/2015

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

SECTION 1 – INTRODUCTION

This Standard describes the security features included in the Tenant Managed Services (TMS) – Basic (formerly the Customer-Owned Equipment Managed Service or COEMS) and TMS – Premium (formerly the Federated Data Center or FDC) offerings provided by the Office of Technology Services (OTech). This Standard applies to the TMS environments from the customer perspective.

SECTION 2 – STANDARD REQUIREMENTS

- A. The TMS offering provides a secure physical location, proper environmental controls, power, and an Internet connection (if requested) for housing tenant-managed equipment within the OTech raised floor environment.
- B. The TMS environment is isolated from the OTech secured network environment. The OTech secured network environment must be protected by firewall technology to restrict inbound and outbound Internet Protocol (IP) traffic to/from the TMS environment.
- C. Virtual Private Networks (VPNs) tunnels are not permitted to connect systems in the TMS environment to systems in the OTech internal network.
- D. Wireless Access Points (WAPs) are not permitted in the TMS environment.
- E. Physical access to the TMS environment must be pre-approved via access lists provided by the customer contact to the OTech Customer Representative or Account Manager.
- F. TMS server cabinets must be locked when not in use. A secondary key must be issued to the OTech Command Center. The OTech Command Center is required to securely store the secondary key. Cabinets found unlocked will be locked upon discovery.
- G. Access to the OTech facilities for TMS customers is stated in 3112 – Tenant Managed Services Access Procedure. TMS customers must adhere to the onsite physical security requirements as stated in the procedure.

SECTION 3 – APPLICABILITY AND EXCLUSIONS

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.

SECTION 4 – AUDITING AND REPORTING

- A. Auditing may be performed at the discretion of the Security Management Branch or its designees. In the event that an audit determines this Standard is not being upheld, 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.
- C. Physical access to the TMS environment may be revoked to anyone who violates this Standard.

SECTION 5 – AUTHORITY/REFERENCES

[3112 - Tenant Managed Services Access Procedure](#)
[Security Policy/Standard Exception Request Form, TECH 358](#)

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