California Department of Technology	3112

TENANT MANAGED SERVICES ACCESS 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

This document covers procedures for Tenant Managed Services – Premium (formerly the Federated Data Center or FDC) and Tenant Managed Services – Basic (formerly the Customer-Owned Equipment Managed Service or COEMS).

The purpose of this procedure is to assist Tenant Managed Services (TMS) customers to gain access to Office of Technology Services (OTech) buildings housing their environments. TMS security requirements are documented in OTech Procedure 3111 – Tenant Managed Services Security Standard.

Controlling physical access to the buildings, computer rooms, and grounds is critical for maintaining a secure computing environment. OTech uses a Security Access System (Badging) to grant access to employees and authorized visitors.

SECTION 2 – STANDARD PROCEDURE

Customers must follow the below procedure to gain access to the OTech facility(s) housing their equipment:

Establishing Authorization

1. The TMS customer department designates their Customer Contact and communicates the designee's name to their OTech Account Manager (AM) or Customer Representative (CR).

2. The Customer Contact will provide the AM or CR an access list of authorized staff and vendors who are permitted to access the customer department's equipment at the OTech.

3. Only the Customer Contact will work with the AM or CR to change the access list.

4. To assure access to those permitted, the AM or CR will create and maintain a standing visitor log containing the names provided by the Customer Contact.

Gaining Access

1. Only individuals on the access list will be able to check-in at the main lobby of the OTech facility. Check-in tasks during normal business hours or off-hours are listed below.
    a. Display valid ID (customer department ID is preferred).
    b. Validate permitting access via the authorized visitor log.

c. Check-in equipment. The security guard may request to inspect backpacks, laptops, hardware devices, etc. at check-in and check-out of the facility.

2. A temporary badge will be issued at the completion of the check-in process. The temporary badge must be returned to the same Security Desk prior to exiting the facility; the badge must never be taken off site.

3. TMS customers and vendors ***must*** be on a visitor log before access can be permitted. TMS customers are unescorted visitors; however, their vendor(s) must be escorted at all times while within the OTech facility.

TMS Customer On-Site Responsibility

TMS customers are responsible for following the on-site security procedures below:

1. Understand the following badge requirements:
   a. Badge must be worn at all times.
   b. Badge must be worn on outer-most garment.
   c. No piggybacking through access doors.
   d. No badge sharing among visitors or providing access with their badge.
   e. Badge in at necessary badge readers.
   f. Only one person at a time at entry points.
   g. Inform your OTech CR or AM who will notify the Security Management Branch if a badge is lost.

2. Since these visits are unescorted, you and your vendor(s) are only permitted access to the area(s) of the raised floor housing your equipment.

3. Surrender your badge, upon departure, to the main Security Desk.

After-Hours Exception

1. If a TMS customer has an emergency during off hours, and a representative who is on the access list needs access to the equipment, they may check in at the front desk as done during normal business hours.

2. If a TMS customer has an emergency during off hours and a representative **not** currently on the access list needs access to the equipment, the Customer Contact may add them to the visitor log by contacting the Service Desk at 916-464-4311. Once the representative has been added to the visitor log, they can gain access to the equipment.

SECTION 3 – APPLICABILITY AND EXCLUSIONS

A. This procedure applies to OTech employees and TMS customers. 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 California Department of Technology Chief Information Security Officer and the reporting employee's immediate supervisor.

SECTION 5 – AUTHORITY/REFERENCES

Security Policy/Standard Exception Request Form, TECH 358
3111 – Tenant Managed Services Security Standard

Please notify your OTech Customer Representative for these documents:
3100 - Asset Protection Policy
Badge/Access Request Form, TECH 255