

 <b>California DEPARTMENT OF TECHNOLOGY</b>		<b>3103</b>	
<b>PHOTOGRAPH REQUEST PROCEDURE</b>			
<b>OWNER:</b>	Administration Division, Facility and Administrative Services Branch	<b>ISSUE DATE:</b>	9/24/2007
<b>DISTRIBUTION:</b>	Office of Technology Services Employees	<b>REVISED DATE:</b>	8/30/2016

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

## SECTION 1 – INTRODUCTION

To ensure that Office of Technology Services (OTech) assets are not disclosed in an inappropriate manner, photographs of OTech assets and the Tenant Managed Services (TMS) environment must be addressed using the information in this Procedure.

Please note that OTech-owned digital cameras must be used to take the photographs; no other cameras (including cell phones) are permitted.

## SECTION 2 – PROCEDURE

### Photograph Requests from External Sources

Employees who are asked to take photographs of property should refer the requester to their Account Representative or the OTech Service Desk.

TMS customers requesting photographs should contact their Account Representative for assistance in submitting a Service Request.

The Service Request must contain the following:

- An itemized list of desired photographs.
- Descriptions that will identify exact hardware, such as make, model, serial number, etc.
- Approval from the Information Security Officer (ISO) for which the data and/or hardware is owned; not necessarily the ISO of the requester.

#### **Customer ISO Responsibilities**

Approve the Service Request via the Customer Service System or provide written authorization to the Account Representative assisting with the request. The Representative will attach the written approval to the Service Request on the ISO's behalf.

#### **Account Representative Responsibilities**

- Ensure that a Service Request has been submitted on behalf of the requester, if necessary.
- Work with the Security Management Branch to obtain customer ISO approval, if necessary.

#### **Security Management Branch Responsibilities**

- Authorize and validate the requester and customer ISO approval.
- Locate requested hardware (with assistance from Computer Room staff).

- Take photographs to ensure appropriateness.
- Download photographs to a secure media, which will be issued to the Account Representative or requester.
- Delete any photographs remaining on the camera upon closure of the request.

### **Photographs for Internal Office of Technology Services Use**

Submit a Remedy Service Request that contains the following information:

- An itemized list of desired photographs.
- Descriptions that will identify exact hardware, such as make, model, serial number, etc.
- Justification and the use for the photographs.

If employees wish to use an OTech camera that is assigned to their technical area, the Security Management Branch will need to authorize the photographs after they are taken.

### **SECTION 3 – APPLICABILITY AND EXCLUSIONS**

- A. This Procedure applies to applicable resources and anyone accessing systems. 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 followed, 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**

[3502 - Information Security Exception Request Procedure](#)  
[Security Policy/Standard Exception Request Form, TECH 358](#)

**Please contact your OTech Customer Representative for the below document:**

3100 - Asset Protection Policy