California DEPARTMENT OF TECHNOLOGY	3138

SYSTEM ADMINISTRATOR ACCESS STANDARD			
OWNER:	Security Management Branch	**ISSUE DATE:**	7/13/2010
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 addresses System Administrator access roles and responsibilities, with respect to Office of Technology Services (OTech) servers.

System Administrator access, for the purposes of this Standard, is defined as the role of a user that allows privileges on the system to access or modify system settings. Commonly, this access is referred to in the Windows environments as "administrator access."

Staff requires administrative access to systems/environments and/or access to databases in order to perform their assigned job responsibilities. Best practices and many compliance standards require formal management authorization for this type of access before it is granted, and formal tracking of this access after it is granted.

SECTION 2 – STANDARD REQUIREMENTS

Part I – System Administrator Standards

The requirements listed below must be implemented to consolidate server security across systems in OTech managed services; they are necessary for OTech system administrators to properly support, administer, and audit the systems.

A. Servers shall be installed and configured by OTech system administrators.

B. Platform and operating system installations shall retain current security rights, as configured by OTech system administrators.

C. Modification to non-customer application server settings will be restricted to OTech system administrators. If specific changes are needed, customers must submit a Service Request requesting the change(s).

D. Support, administration, and auditing of the servers are performed by OTech staff. The requirements listed below must be implemented to consolidate system security and integrity. Additionally, OTech's business model requires that environments be standardized in order to achieve cost efficiencies.

OTech system administrators are responsible for:

- Maintaining, scheduling, and installing operating system, security updates and health of the servers in accordance with 3302 – Security Update Management Standard.
- Maintaining system hardening configurations in accordance with 3126 – Server Security Standard and 3130 – Device Ports and Protocols Security Standard.
- Server access accounts. Only OTech system administrators are authorized to change access privileges.
- Service accounts and their respective access rights for any server management software system in accordance with 3122 – Password Standard.

E. Customers shall be granted permissions to their servers, as needed, to perform application maintenance.

F. Applications must have specific roles and/or user permissions, as needed, to perform application functions.

Part II – System Administrator Parameters

Customers with elevated access permissions are not permitted to perform the following actions without prior approval and coordination from the appropriate OTech service area:

A. Changes to the operating system or non-customer application configuration parameters at the time of system turnover.

B. Changes to OTech-scheduled management or patching functions.

C. Creation or modification of user accounts.

D. Changes to, or deletion of, service accounts and OTech system administrator accounts (these accounts are owned by OTech staff).

E. Installation or configuration of services and components that block or impede OTech system administrators from supporting the server.

F. Adhere to the 3132 – Midrange Database Server Security Standard for additional system administrator parameters for database servers.

Part III – System Administrator Responsibilities

Users with elevated access permissions must not:

A. Use the privileged account for any purpose that can be accomplished using a less privileged account.

B. Use the server for any purpose that is more appropriately accomplished on a workstation, such as code development or document creation.

C. Use the server as a way of avoiding various restrictions that are placed on workstations, such as browsing Web sites normally restricted on OTech workstations, or installation of unlicensed or pirated software.

Part IV – Requesting Elevated System Access Permissions

OTech customers may be provided elevated access permissions to the servers for which their applications are installed. Customers must submit a Service Request to obtain elevated access permissions. Include the following information in the request:

A. The names of the users requiring the access.

B. Names of the servers for which access is being requested.

C. Detailed listing of the specific access requested. If any request includes system permissions that are normally restricted to an OTech database or web server managed services, a technical justification must be submitted with the request.

D. Approval from the data owner's Information Security Officer (ISO).

The Service Request may be granted for up to one year from the time that it is approved by OTech. Changes to an existing request or extensions must be submitted via a supplemental Service Request.

SECTION 3 – APPLICABILITY AND EXCLUSIONS

A. This Standard is ***not*** applicable to the UNIX and Linux and mainframe platforms. Tasks on these platforms that require elevated access permissions require a Service Request. Upon receiving the Service Request, an OTech System Administrator will initiate a meet-and-confer with the requestor to accomplish the task on the customer's behalf.

B. This Standard is applicable to internal staff and external customers with applications in OTech managed services that require elevated system access. Direct any questions regarding the applicability of this Standard to the Security Management Branch for clarification.

C. This Standard does ***not*** apply to Tenant Managed Services (TMS) customers.

D. Exceptions to this Standard must be documented and will be considered on a case-by-case basis.

E. Server modifications made by customers with elevated access permissions may affect OTech's ability to provide secure system environments, troubleshooting, and service restoration. The customer assumes increased responsibility and risk for system security, support, troubleshooting, and service restoration. Requests for OTech assistance will result in additional consulting charges and will be performed only if OTech staff is available to troubleshoot.

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(s) for remediation, including the system administrator's Information Security Officer, and system administrator access will be revoked until remediation has been completed by the customer.

B. Any known violations of this Standard must be reported to the California Department of Technology Information Security Officer and the reporting employee's immediate supervisor. Noncompliance with the requirements outlined above may result in permanent revocation of system administrator access.

SECTION 5 – AUTHORITY/REFERENCES

3132 - Midrange Database Server Security Standard
3502 - Information Security Exception Request Procedure
Security Policy/Standard Exception Request Form, TECH 358
Service Request

Please contact your OTech Account Representative for the below documents:
3100 - Asset Protection Policy
3122 - Password Standard
3126 - Server Security Standard
3130 - Device Ports and Protocols Security Standard
3302 - Security Update Management Standard