SUBJECT:	**Privileged Access to Information Systems**	**NUMBER:**	**107-004-140**
DIVISION:	**Chief Information Office**	**EFFECTIVE DATE:**	**July 10, 2013**

APPROVED:
Michael Jordan, Director *(signature on file with DAS Business Services)*

POLICY/ PURPOSE: This policy establishes the process and expectations for granting and using privileged access to the information systems of the State Data Center (SDC). Privileged access enables users to take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators, staff who perform computing account-administration, or other staff whose job duties require special privileges over a computing system or network.

AUTHORITY: Statewide Policy #107-004-110: Acceptable Use of State Information Assets
ORS 182.122: Information Systems Security in Executive Department

APPLICABILITY: This policy applies to all SDC users and contractors, and staff and contractors of customer-agencies who require, request, and acquire privileged access to the SDC's information systems.

ATTACHMENTS: Attachment A: Privileged Access Request
Attachment B: Privileged Access Agreement

DEFINITIONS:

Authorized Requestor – A person delegated by an agency who is authorized to approve and submit user requests for privileged access.

Compelling Circumstances – Circumstances in which failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or state policy, or significant liability to the SDC or its customers.

Electronic Communications – Any transfer of signals, writings, images, sounds, data or intelligence that is created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or more electronic communication systems. Under this policy, an electronic file that has not been transmitted is not an electronic communication. (This definition is modeled after the Electronic Communications Privacy Act (US Code Title 18 § 2510).

Electronic Communications Records – The contents of electronic communications created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or more electronic communications systems or services. This definition applies to original records, copies, or modifications of original records, and includes attachments to electronic communications records and transactional information associated with such records.

Electronic Communications Systems or Services – Any system used to message, collaborate, publish, broadcast, or distribute, which depends on electronic communications resources to create, send, forward, reply to, transmit, distribute, broadcast, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network-systems between or among users or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes.

User, End-User – People who use IT services on a day-to-day basis. Users are distinct from customers, as some customers do not use the IT services directly.

Holder of an Electronic Communications Record – A user of electronic communications who, at a given point in time, receives or possesses a particular electronic communications record. This definition applies whether or not the user is the original creator of the record. Also see "Possession of Electronic Communications Record," below.

Information Systems – Computers, hardware, software, storage media, networks, and the operational procedures and processes used to collect, process, store, share or distribute information — beyond ordinary public access — within the state's shared computing and network infrastructure.

Possession of Electronic Communications Record – A person possesses an electronic communications record when he or she has effective control over the location of its storage or access to its content. Example: Under this policy, an electronic communications record that resides on an electronic communications server awaiting download to an addressee is in the possession of that addressee. This definition does not apply to system administrators and other operators of SDC electronic communications services with regard to electronic communications not specifically created by or addressed to them.

Privileged Access – Access to an information system that enables the user to take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access implies greater access than the average end-user.

Transactional Information – Information, including electronically gathered information, needed to complete or identify an electronic communication. Examples include but are not limited to electronic mail headers, summaries, addresses and addressees.

GUIDELINES:

I. Overview

The SDC grants privileged access to SDC information systems based on the job requirements of requestors, according to the following scenarios:

a) A user requires access over an extended period of time from a known location or locations. The SDC grants administrative credentials to the user via this policy. In addition, appropriate firewall rules will be set up to allow access for the necessary tools, e.g. SSH, RDP, to permit the user to access the systems, devices, and data outlined in the user's Privileged Access Agreement.

b) A user requires access over an extended period of time from possibly varying locations. The SDC grants administrative credentials to the user via this policy. In addition, the SDC will create a VPN account for the user that includes filters to allow access for the necessary tools, e.g. SSH, RDP, to permit the user to access the systems and devices outlined in the user's Privileged Access Agreement.

c) A customer requires ad-hoc access, such as for technical support or for initial application configuration. An SDC technician creates a conference session to allow one or more remote users to share a session. The technician connects to the device that needs to be shared, using his or her credentials, and shares the window with the remote party. The technician stays present to monitor the changes being made and closes the session after the work is completed. Optionally, the technician may record the session to create a record of the changes made.

II. Expectations and Requirements

a) Users with privileged access must respect the rights of system users, respect the integrity of systems and related physical resources, and comply with relevant laws and regulations.

b) Users with privileged access have an obligation to keep themselves informed regarding any procedures, business practices, policies and operational guidelines pertaining to the activities of their local department. In particular, the principles of privacy of information hold important implications for system administration at the SDC.

c) Privileged access applies to a particular period of time and includes only specific tasks. Time periods are based on the required tasks; the time period may be brief, such as one-time access, intermittent access, or longer.

d) Privileged access will end at the close of the time period granted by the SDC.

e) It is the customer agency's responsibility to immediately inform the SDC every time an employee leaves, changes dutie3s or no longer needs privileged access to perform their current job duties.

f) The SDC will perform a review twice a year or at least 180 days to verify that accounts are still active. The SDC shall provide a list of inactive and expired accounts to customer agencies. It is the customer agency's responsibility to review the list of exceptions and to notify the SDC within 30 days, when list of exceptions received, of any modifications or else the SDC will revoke access.

g) People approved for privileged access will have two user IDs: one for normal day-to-day activities and one to perform administrator duties.

h) Users with privileged access may only use their access to perform the tasks and functions outlined in the user's Privileged Access Agreement. Any other use including viewing, modifying, copying, disclosing or destroying a system or other user's data, is unauthorized.

i) Users must receive approval from the SDC Change Control Board before making changes to production systems. This does not apply to changes in test or development systems.

j) An agency must communicate directly with its privileged access users if the agency has special requirements, including documentation, related to confidentiality and secrecy.

k) Electronic communications users are not responsible for electronic communications records in their possession when they have no knowledge of the existence or contents of such records.

l) The SDC grants privileged access to users exclusively for the performance of their day-to-day job duties.

m) A Privileged Access Agreement for System Administrators (i.e., the privileged access individual user agreement) shall be signed and submitted to the SDC before the SDC shall grant privileged access to the requesting user.

n) An agency CIO and/or Authorized Requestors shall approve and submit a request for privileged access.

DAS DEPARTMENT OF ADMINISTRATIVE SERVICES
STATE DATA CENTER

Attachment A: Privileged Access Request

Type of Request: □ Add User □ Modify User Access □ Revoke User Access	**Special Needs:** □ Temporary Access until (date): □ Other:	**User Status:** □ Permanent Employee □ Temporary Employee □ Contractor □ Vendor

User Information

Agency (if vendor or contractor, specify the affiliated agency) **Name:** First M.I. Last	Applicable User ID	Effective Date	
Work Unit	Position/Title		
E-mail Address	Phone/Ext.	Notes	
Physical Work Address (Include Suite or Floor as applicable)	City	State	Zip

User Access Information

Which SDC domain do you require access to (e.g. Distributed, iSeries, UNIX, Mainframe, etc.)?
What business reason can you provide to support your request? Please be specific.
Which systems or devices will you require access to?

Approvals

Customer Appointed CIO or Authorized Requestor

Name: First M.I. Last	Phone/Ext.	Area (description)	Today's Date

Customer Approving Manager

Name: First M.I. Last	Phone/Ext.	Area (description)	Today's Date

Employee

Name: First M.I. Last	Phone/Ext.	Area (description)	Today's Date

SDC Approving Domain Manager or Delegate

Name: First M.I. Last	Phone/Ext.	Domain Area (description)	Today's Date

DAS DEPARTMENT OF ADMINISTRATIVE SERVICES
STATE DATA CENTER

Attachment A: Privileged Access Request

SDC Division Administrator or Delegate

Name: First M.I. Last	Phone/Ext.	Domain Area (description)	Today's Date

Denials

The SDC cannot grant the access request for the following reason:

Please refer any questions about this denial to:

Name: First M.I. Last	Phone/Ext.	Domain Area (description)	Today's Date

Contact: sdc.servicedesk@state.or.us

DAS DEPARTMENT OF ADMINISTRATIVE SERVICES
STATE DATA CENTER

Attachment B: Privileged Access Agreement

INTRODUCTION

Privileged access to the information systems of the State Data Center (SDC) enables a user to take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators, staff who perform computing account- administration, or other staff whose job duties require special privileges over a computing system or network.

Users with privileged access must respect the rights of system users, respect the integrity of systems and related physical resources, and comply with relevant laws and regulations. Users also have an obligation to keep themselves informed regarding any procedures, business practices, policies and operational guidelines pertaining to the activities of their local department.

In particular, the principles of privacy of information hold important implications for computer system administration at the SDC. Users with privileged access must comply with applicable policies, laws, regulations, precedents, and procedures, and must pursue only appropriate action — the actions required to provide high quality, timely, reliable computing services.

GENERAL PROVISIONS

1. This agreement shall be read and signed before the SDC shall grant privileged access to the user.
2. If a user can accomplish a task without using privileged access, they should do so unless the burden of time or other resources require use of privileged access.
3. Users may only use privileged access to perform assigned job duties on the machines and networks outlined in this agreement. A user's assigned work may include standard system-related duties, such as:
    a. Installing system software
    b. Relocating users' files from critically overloaded locations
    c. Performing repairs that are required to return a system to normal function, such as fixing files or file processes, or killing runaway processes
    d. Running security checking programs
    e. Monitoring the system to ensure reliability and security
    f. Modifying network device configurations
    g. Changing firewall rules
4. Users may use privileged access to grant, change, or deny the resources, access, or privileges of another user, but only for authorized account-management activities or under exceptional circumstances. Such actions must follow any existing organizational guidelines and procedures. Examples include:
    a. Disabling an account apparently responsible for serious misuse such as: attempting to compromise root (UNIX) or the administrator account (Windows), using a host to send harassing or threatening e-mail, using software to mount attacks on other hosts, or engaging in activities designed to disrupt the functioning of the host itself
    b. Disconnecting a host or subnet from the network when a security compromise is suspected
    c. Accessing files for law enforcement authorities with a valid subpoena
5. In the absence of compelling circumstances (see the definitions section of SDC Policy 107-027-010, Privileged Access), the investigation of information in, or suspension of, an account suspected to be compromised should be delayed until normal business hours to allow appropriate authorization and notification activities.

a. In all cases, users with privileged access must limit their perusal of other users' electronic information to the least amount necessary, and take the least action necessary to resolve a situation.

b. Users with privileged access must take necessary precautions to protect the confidentiality of information encountered in the performance of their duties.

If users with privileged access inadvertently see information that indicates serious misuse, they must immediately consult their supervisor. If the situation is an emergency, intervening action may be appropriate.

RECOURSE

If conflicts or disputes arise regarding activities related to this agreement, users may pursue their rights to resolve the situation through existing procedures. Examples: informal supervisory or department conflict-resolution procedures, relevant provisions of employment policies or contracts, student or faculty conduct procedures, or other documents that pertain to the particular user's affiliation with the SDC.

AGREEMENT

- I have read this *Privileged Access Agreement* and the state policy on Acceptable Use of State Information Assets (#107-004-110).
- I agree to comply with the provisions of this *Privileged Access Agreement* and the state policy on Acceptable Use of State Information Assets.

Agency CIO or Delegate Signature _____

Print Name _____

Agency/Department _____

Date _____

Agency Authorized Requestor(s) Who Can Approve Privileged Access Users:
(Print Name Clearly)

_____

SDC Authorizing Signature _____

Print Name _____

SDC Receipt Date _____