



OREGON STATE DATA CENTER



Service Level Agreement



Approved on 2/17/2010



(503) 373-1000

E-mail SDC_ServiceDesk@state.or.us

DAS
DEPARTMENT OF
ADMINISTRATIVE
SERVICES

TABLE OF CONTENTS

1	Introduction	1
1.1	Associated Documents.....	1
1.2	Service Period (Start, End, Review).....	1
2	Common Service Levels	2
2.1	Service Description	2
3	Computing.....	6
3.1	Dedicated Distributed Systems Hosting Environments	6
3.2	Dedicated Remote Distributed Systems Hosting Environments	7
3.3	Mid-range Based Application Server Service.....	9
3.4	Mid-range Based Database Service.....	11
3.5	Mid-range Based Dedicated UNIX Hosting Service	12
3.6	Mid-range Based Dedicated i-Series Hosting Service	13
3.7	zOS Hosting Environment	15
3.8	z/LINUX Hosting Environment.....	16
3.9	Backup and Restore Services	18
4	Network and Security	20
4.1	Wide Area Network Services (WAN).....	20
4.2	State Mall Area Network.....	21
4.3	Local Area Network Services (LAN).....	22
4.4	Network Support Services – DHCP and/or DNS.....	23
4.5	Remote Access Virtual Private Network (VPN).....	25
4.6	Site to Site Virtual Private Network (VPN).....	26
4.7	Firewall Management	27
4.8	Email Hub Services	28
4.9	State E-mail Directory Synchronization.....	29
5	Voice	30
5.1	Traditional Phone Systems	31
5.2	Voice Over IP (VOIP) Phone Systems	33
6	Appendix	35
6.1	Definitions.....	35

1 Introduction

The purpose of the Service Level Agreement (SLA) is to document the expectations and responsibilities of the Oregon State Data Center (SDC) and the agency hereafter referred to as 'customer'. This document identifies service levels provided by the SDC. The document is not meant to be static, but a working document that reflects the continuous change in services, process, and expectations between the State Data Center and its customers. The SDC will support all systems within its scope. These Service Level agreements are to set expectations for services supported within the SDC standard configurations, and non-standard systems will be supported with best effort available.

1.1 Associated Documents

As additional documentation is reviewed and approved by the SDC advisory committees, it is released and available at www.oregon.gov/DAS/SDC.

- [Service Catalog](#) – Services referred to in this document are defined in detail in the Oregon State Data Center Services Catalog.
- [Scope Matrix](#) – Roles and Responsibilities for services provided by the State Data Center and by the Agency customers are documented in the approved Scope Matrix.
- Scope [Inclusion/Exclusion](#) Process – The process to include new services in or exclude systems from the SDC scope.
- SDC Technical Standards – Standards for hardware and software supported by the SDC.
- [SDC Process Documentations](#) – Process and procedures for services provided are documented in the SDC library and are available upon request. Processes in use and under development include:
 - [Change Management](#)
 - Incident and Problem Management
 - Release Management
 - [Asset Management](#)
 - [Request Fulfillment](#)
 - Service Level Management
 - Account Management
 - Procurement and Financial Assessments
 - Capacity Management
 - Security and Physical Access Management

1.2 Service Period (Start, End, Review)

This agreement is in effect from the date of signing through December 31, 2011 or until canceled, modified, or replaced. The review of the agreement will begin 45 days prior to the agreement expiration. Future agreements will be written for one biennium.

_____ SDC Administrator _____ Date

_____ Agency CIO _____ Date

2 Common Service Levels

This section describes the common service levels for all services provided by the SDC. Service specific additions and or exceptions are described for each service in the sections following.

2.1 Service Description

In this section of each service below there will be a brief description from the Service Catalog of what the service is.

2.1.1 SDC Standard

In this section of each service below there will be a description of the standard configuration that is subject to all of the service levels for that service. Systems not within the standards will be supported on a “Best Effort” basis.

2.1.2 Scheduled Maintenance

2.1.2.1 Standard Maintenance Window

If scheduled maintenance is required, the SDC will use the standard maintenance window. This window will only be used when needed. Use of this window will be governed by the SDC change management process. Emergency changes required to restore services can be made outside of the maintenance window.

2.1.2.2 Patching

Patching descriptions and schedules are specific to each service, so details are provided below.

2.1.2.3 Change Management

Information regarding scheduled changes will be available through the SDC Support System (S³) web site: <https://www.oregonsdc.org/>

- *Customers will be allowed at least 2 business days to provide questions, concerns or comments on scheduled changes so that adjustments to those changes may be made.*
- *All high risk / high impact changes will provide at least 10 business days notification prior to change execution.*

In order for the SDC to better coordinate activities in production environments, customers are asked to schedule application maintenance with potential impact to the SDC outside the SDC maintenance windows, and notify the SDC prior to changes to application in agency production environments. The SDC requests to be notified at least three business days prior to any planned application maintenance in production environments. If the customer requires planned application maintenance during an SDC maintenance window, they must send a request to the SDC Change Manager at least 9 business days prior to the requested date. This will allow the SDC to assess the impact to the scheduled changes and possibly reschedule certain changes.

2.1.3 Service Disruption

2.1.3.1 Monitoring

If the SDC monitoring system notifies that a system is unavailable, the SDC will respond to the Service Disruption without action from the customer. The customer will be informed about

SDC Service Level Agreement

outages through the SDC Service Disruption procedures. The basic monitoring reports up/down status for the device.

2.1.3.2 Communications / Time to Respond

Staff will acknowledge customer requests and provides initial contact to gather requirements within the following response times:

- *Severity 1 – 90% within 15 minutes **
- *Severity 2 – 90% within 30 minutes.*
- *Severity 3 – 95% within 1 day.*
- *Severity 4 – 95% within 2 days.*

Service Disruption – Refer to standards for Incident Management for more information on service disruption handling.

2.1.3.3 Time to Restore

The SDC will restore services within the target resolution times set in the Incident Management Severity Level Response chart at the following rates:

- *Severity 1 – 70% within 2 hours.**
- *Severity 2 – 75% within 4 hours.*
- *Severity 3 – 90% within 2 days.*
- *Severity 4 – 95% within 5 days.*

2.1.3.4 Escalations

Service disruptions will escalate to the next higher severity as the target resolution time for the current severity level is exceeded or is expected to exceed resolution time.

*Refer to Incident Management standards for more information on service disruption handling including target response times and target resolution times.

2.1.4 Security

The SDC provides protection of agency resources at all levels of data classification. Firewalls are implemented and managed, as necessary, to provide separation and restriction between devices. When requested encryption can be provided to securely transmit data. Intrusion detection is implemented at key points in the network to alert on and restrict malicious traffic.

2.1.4.1 Intrusion Detection

The SDC provides Network Intrusion Detection that examines traffic as it passes defined points on the network to see if it matches “signatures” of known malicious activity. This applies to network intrusion detection only, and does not include host intrusion detection. Host intrusion detection is not currently provided, but may be provided in the future.

2.1.4.2 Security Incident Response

The SDC will notify ESO and agency security personnel of intrusion incidents and suspicious activities in accordance with the SDC and agency Security Incident Response Plan. The agency must designate who will receive these types of notifications.

2.1.4.3 Privileged Access

Privileged access to SDC systems is limited. The SDC will manage privileged access to systems granting access to only those whose job duties require it. Customers are not given privileged access without special authorization. If methods other than using privileged access will accomplish an action, those other methods must be used unless the burden of time or other

resources required clearly justifies granting privileged access. The privileged access process can be found on the SDC Support System (S³) web site: <https://www.oregonsdc.org/>

2.1.5 Availability

Availability is calculated monthly in the following manner:

$$\text{Availability}\% = (\text{Total Service Hours} - \text{Down Time}) / (\text{Total Service Hours})$$

Down Time will be calculated from the SDC Request Tracker (RT) system as a sum of all of the downtime recorded for each service disruption.

2.1.6 Request Fulfillment

SDC Engineering requests for new environments or major upgrades are fulfilled in priority order. The SDC allows the customer to prioritize engineering requests. Customers set priorities for SDC Engineering Requests through their SDC Account Manager. Frequent changes to engineering priorities can reduce the SDC's ability to deliver these requests on time, so major reprioritization should occur no more frequently than once per month. Minor changes due to the completion of prioritized requests can be addressed at any time.

Once the SDC and the customer agree on the requirements and the SDC determines the solution design for the request, the SDC will provide the customer an expected delivery date (Due Date). If the requirements and/or the solution design changes, then the Expected Delivery Date may change. The customer will be notified prior to any change to the Expected Delivery Date. The SDC will deliver **90%** of the requests within a **20%** variance of the Expected Delivery Date. (e.g. If the Expected Delivery Date is **30** days from the request submit date, then the SDC will deliver the request within **6** days of the Expected Delivery Date.)

SDC Standard Work requests are fulfilled in order of receipt. Most requests are completed within one week depending on the nature of each request and the volume of requests to the SDC.

2.1.6.1 Communications

Staff will acknowledge customer requests and provides initial contact to gather requirements within the following response times:

- *Standard Work – 90% within 3 business days*
- *Engineering Required – 90% within 3 business days*

2.1.7 Service Continuity

Continuity ensures that in the case of a catastrophic failure, the service can be restored within an agreed upon period. Disaster Recovery services can be added to this service at an additional cost.

In the case of a catastrophic issue in which a hardware failure requires replacement, additional time may be required to procure replacement hardware and/or repurpose and reload hardware within the SDC. The incident management process will be used for communications in this event.

The SDC will provide best effort to restore systems to service that are end-of-life or do not conform to the SDC Standards in the event of a catastrophic failure.

2.1.8 Reporting

The SDC will make the Service Level Measurements available to the customer at the end of each month. Quarterly Service Level reports will be made available that show the Service Level Measurements across the entire SDC and Annual reports will be made available during the annual review the Service Level Agreement.

SDC Service Level Agreement

2.1.9 Remedies

The SDC will review the service levels for all services. If the SDC does not meet a service level for a particular month, then the Service Level Manager will analyze the root cause within 30 days and determine if a Service Improvement Plan is required. The initial analysis will be made available to the affected customer(s) and included in an annual report. Service Improvement Plans will be provided to the customer(s) upon completion within 90 days after analysis.

Intro and Common Service Level Revision History

Date	Author	Description of change
9/8/09	Sean McMullen	Created a common service levels section.
10/29/09	Sean McMullen	Changed lead time for high risk changes to 9 business days.
11/2/09	Sean McMullen	Added target numbers for Service Disruption and Communications.
11/4/09	Sean McMullen	Added Introduction and Clarifying language to Change Management sections from MF review.
12/14/09	Sean McMullen	Updated Change Section 2.1.2.3 Change Management and 2.1.3 Service Disruption based on CIO feedback.

3 Computing

SDC Computing Services include the procurement, installation, management, and versioning of hardware and software resources required by customers to run custom and licensed applications.

3.1 *Dedicated Distributed Systems Hosting Environments*

Dedicated Distributed Systems Hosting Environment service offering ensures end-to-end delivery of a stable, hosting environment through the entire lifecycle of the deployment. Disaster recovery systems, which may be requested, are not included by default.

3.1.1 SDC Standard

Dedicated Distributed Systems Hosting Environment service offering relate to the specific type of platform architecture selected. Only current or one-past generation Microsoft Windows family systems, current or one-past generation Suse Linux Enterprise Server (SLES), or the currently supported version Netware operating system running on SDC supported hardware are included as part of this service offering. Dedicated hosting environments deploy standalone systems, which do not have automated failover solutions. These hosting environments, therefore, contain at least one single-point-of-failure at a critical tier (i.e. at the application server tier, the database tier, or in terms of networking). Dedicated hosting does not include technical support for the business applications installed in these environments.

3.1.2 Scheduled Maintenance

3.1.2.1 Standard Maintenance Window

Monday - Thurs 10 p.m. 2 a.m.

Sunday 6 p.m. Midnight

3.1.2.2 Patching

The SDC manages patching on a monthly schedule. Patching is normally applied during the scheduled maintenance window above. Below is a breakdown of our schedule based on the week of the month:

- *2nd Tuesday (or 2nd week of the month) of the month - Microsoft Patch Tuesday. The day after these patches are released we will send a notification to the Agency Patch Management distribution group. The e-mail will contain information about the specific patches and the planned distribution dates.*
- *On the 3rd week of the month - We will notify our "1st Stage Test Deployment Group" and release patches to these machines as planned in the Change Management schedule and during the agencies planned maintenance period.*
- *On the 4th week of the month – We will release patches as planned in the Change Management schedule and during the agencies planned maintenance period.*
- *On the 5th / 1st week of the month – Coordination with agency staff on the remediation of patch distributions that failed to install.*

Exceptions to the normal schedule can be requested, and emergency critical patches will follow the Urgent or Emergency Change Management process.

3.1.3 Service Disruption

3.1.3.1 Monitoring

In addition to the basic monitoring, dedicated windows distributed systems hosting environments also monitor the following items for errors or defined alarm thresholds:

- *Memory/Page file*
- *Operating System Volume (Physical/Logical Disk)*
- *Network Interface*
- *Processor*

Enhanced monitoring of critical servers is available upon request.

3.1.4 Security

Refer to the common section above.

3.1.5 Availability

Availability for the windows distributed systems dedicated hosting is the percent of time the hosting environment servers are available, including accessibility and functionality of the operating system during the hours of service (excluding maintenance windows). Dedicated Distributed Systems Hosting Environment availability includes the core network components, but does not include wide-area network components.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

Dedicated Distributed Systems Hosting Environments will be available **99.9%** each month.

3.1.6 Request Fulfillment

Most dedicated windows / Linux hosting environments can be delivered in thirty days. Some environments may take more or less time depending on complexity.

3.1.7 Service Continuity

For systems within the SDC standard, the system will be restored within 48 hours.

3.1.8 Reporting

Refer to the common section above.

3.1.9 Remedies

Refer to the common section above.

3.2 *Dedicated Remote Distributed Systems Hosting Environments*

Dedicated Remote Hosting Environment service offering ensures end-to-end delivery of a stable, back-end hosting environment through the entire lifecycle of the deployment. Disaster recovery systems, which may be requested, are not included by default.

3.2.1 SDC Standard

Dedicated Remote Distributed Systems Hosting Environment service offering relate to the specific type of platform architecture selected. Only current or one-past generation Microsoft Windows family systems, current or one-past generation Suse Linux Enterprise Server (SLES), or the currently

supported version Netware operating system running on SDC supported hardware are included as part of this service offering. Dedicated hosting environments deploy standalone systems, which do not have automated failover solutions. These hosting environments, therefore, contain at least one single-point-of-failure at a critical tier (i.e. at the application server tier, the database tier, or in terms of networking). Dedicated hosting does not include technical support for the business applications installed in these environments. Power to the remote equipment, including conditioning and uninterruptible power sources, is not included in this service.

3.2.2 Scheduled Maintenance

3.2.2.1 Standard Maintenance Window

Monday - Thurs 10 p.m. 2 a.m.

Sunday 6 p.m. Midnight

3.2.2.2 Patching

The SDC manages patching on a monthly schedule. Patching is normally applied during the scheduled maintenance window above. Below is a breakdown of our schedule based on the week of the month:

- *2nd Tuesday (or 2nd week of the month) of the month - Microsoft Patch Tuesday. The day after these patches are released we will send a notification to the Agency Patch Management distribution group. The e-mail will contain information about the specific patches and the planned distribution dates.*
- *On the 3rd week of the month - We will notify our "1st Stage Test Deployment Group" and release patches to these machines as planned in the Change Management schedule and during the agencies planned maintenance period.*
- *On the 4th week of the month – We will release patches as planned in the Change Management schedule and during the agencies planned maintenance period.*
- *On the 5th / 1st week of the month – Coordination with agency staff on the remediation of patch distributions that failed to install.*

Exceptions to the normal schedule can be requested, and emergency critical patches will follow the Urgent or Emergency Change Management process.

3.2.3 Service Disruption

3.2.3.1 Monitoring

In addition to the basic monitoring, dedicated windows hosting environments also monitor the following items for errors or defined alarm thresholds:

- *Memory/Page file*
- *Operating System Volume (Physical/Logical Disk)*
- *Network Interface*
- *Processor*

Enhanced monitoring of critical servers is available upon request.

3.2.4 Security

Refer to the common section above.

3.2.5 Availability

Availability for the dedicated remote distributed systems hosting is the percent of time the hosting environment servers are available, including accessibility and functionality of the operating system during the hours of service (excluding maintenance windows). Dedicated Windows / Linux Hosting Environment availability includes the core network components, but does not include wide-area network components.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

Dedicated Remote Distributed Systems Hosting Environments will be available **99.0%** each month.

3.2.6 Request Fulfillment

Most dedicated remote distributed systems hosting environments can be delivered in thirty days. Some environments may take more or less time depending on complexity.

3.2.7 Service Continuity

For systems within the SDC standard, the system will be restored within 72 hours depending on location and weather. (See the Remote Site Support Plan in Appendix C of the SDC Service Catalog for details.)

3.2.8 Reporting

Refer to the common section above.

3.2.9 Remedies

Refer to the common section above.

Distributed Systems Revision History

Date	Author	Description of change
5/20/2009	Sean McMullen	Initial Draft
6/1/09	Sean McMullen	Completed changes from Management and Team Lead reviews.
9/1/09	Sean McMullen	Added boilerplate changes from Security and Network workgroups.
9/22/09	Sean McMullen	Added changes from SDC Internal Review.
9/29/09	Sean McMullen	Added changes from External Workgroup Review

3.3 *Mid-range Based Application Server Service*

The SDC can provide various web and application servers on available platforms. An application server is a software product that presents a user a package of functions built from programs or modules.

The SDC will accommodate agency needs including:

- *Assisting the agency with setting up connections to data sources*
- *Setting up virtual web servers*
- *Granting access as appropriate*

3.3.1 SDC Standard

Mid-range Based Application Server service offering relate to the specific type of application server selected. Only current or one-past generation Oracle Application Server, WebSphere Application Server, or ColdFusion running in a shared environment on SDC supported hardware are included as part of this service offering.

3.3.2 Scheduled Maintenance

3.3.2.1 Standard Maintenance Window

If maintenance is required, the SDC will use the standard maintenance window. This window will only be used when needed. Use of this window will be governed by the SDC change management process.

Monday - Thurs 10 p.m. 2 a.m.

Sunday 6 p.m. 2 a.m.

3.3.2.2 Patching

Patching is done quarterly as needed. All patching is scheduled through the Change Management process, but exceptions to the normal schedule can be requested. Emergency critical patches will follow the Urgent or Emergency Change Management process.

3.3.2.3 Privileged Access

Due to the shared nature of the enterprise shared services environment that hosts these application servers, the SDC cannot grant privileged system access to these environments.

3.3.3 Service Disruption

Refer to the common section above.

3.3.4 Security

Refer to the common section above.

3.3.5 Availability

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

Mid-range Based Application Server services will be available **99.9%** each month.

3.3.6 Request Fulfillment

Most new Mid-range Application Server services can be delivered in 30 days. Some environments may take more or less time depending on complexity. Modifications to the agencies existing services are usually are SDC Standard Work.

3.3.7 Service Continuity

For systems within the SDC standard, the system will be restored within 48 hours.

3.3.8 Reporting

Refer to the common section above.

3.3.9 Remedies

Refer to the common section above.

Midrange AS Revision History

Date	Author	Description of change
9/28/09	Sean McMullen	Initial Draft from internal review.

3.4 Mid-range Based Database Service

The Mid-range Based Database services are provided in an enterprise shared services environment. The SDC support includes:

- *Management of DBA privileges and DBA access.*
- *Definition and management of physical resources needed by product (i.e., buffer pools, catalogs, log files, and archive files.*
- *Providing storage space for database use.*
- *Coordination of scheduling or arranging for database backup and restore jobs to/from tape.*

3.4.1 SDC Standard

Mid-range Based Database service offerings relate to the specific type of platform database selected. Only current or one-past generation Oracle, DB2 and Sybase running in a shared environment on SDC supported hardware are included as part of this service offering.

3.4.2 Scheduled Maintenance

3.4.2.1 Standard Maintenance Window

If maintenance is required, the SDC will use the standard maintenance window. This window will only be used when needed. Use of this window will be governed by the SDC change management process.

Monday - Thurs 10 p.m. 2 a.m.

Sunday 6 p.m. 2 a.m.

3.4.2.2 Patching

Patching is done quarterly as needed. All patching is scheduled through the Change Management process, but exceptions to the normal schedule can be requested. Emergency critical patches will follow the Urgent or Emergency Change Management process.

3.4.2.3 Privileged Access

The SDC will grant DataBase Administrator (DBA) access through the SDC Privileged Access process. Due to the shared nature of the enterprise shared services environment that hosts these databases, the SDC cannot grant privileged system access to these environments.

3.4.3 Service Disruption

Refer to the common section above.

3.4.4 Security

Refer to the common section above.

3.4.5 Availability

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

Mid-range Based Database services will be available **99.9%** each month.

3.4.6 Request Fulfillment

Most Mid-range Based Database services can be delivered in 30 days. Some environments may take more or less time depending on complexity. Modifications to the agencies existing services are usually are SDC Standard Work.

3.4.7 Service Continuity

For systems within the SDC standard, the system will be restored within 48 hours.

3.4.8 Reporting

Refer to the common section above.

3.4.9 Remedies

Refer to the common section above.

Midrange Db Revision History

Date	Author	Description of change
5/20/2009	Sean McMullen	Initial Draft
6/1/09	Sean McMullen	Completed changes from Management and Team Lead reviews.
9/28/09	Sean McMullen	Added Changes from internal review.

3.5 *Mid-range Based Dedicated UNIX Hosting Service*

Dedicated UNIX Hosting Environment service offering ensures end-to-end delivery of a stable, enterprise hosting environment through the entire lifecycle of the deployment. Disaster recovery systems, which may be requested, are not included by default.

3.5.1 SDC Standard

Mid-range Based UNIX Hosting service offering relate to the specific type of platform. Only two generations of the AIX operating system on SDC supported hardware are included as part of this service offering.

3.5.2 Scheduled Maintenance

3.5.2.1 Standard Maintenance Window

If maintenance is required, the SDC will use the standard maintenance window. This window will only be used when needed. Use of this window will be governed by the SDC change management process.

Monday - Thurs 10 p.m. 2 a.m.

Sunday 6 p.m. 2 a.m.

3.5.2.2 Patching

Patching is done quarterly as needed. All patching is scheduled through the Change Management process, but exceptions to the normal schedule can be requested. Emergency critical patches will follow the Urgent or Emergency Change Management process.

3.5.2.3 Privileged Access

Refer to the common section above.

3.5.3 Service Disruption

Refer to the common section above.

3.5.4 Security

Refer to the common section above.

3.5.5 Availability

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

Mid-range Based Dedicated UNIX Hosting services will be available **99.9%** each month.

3.5.6 Request Fulfillment

Most new Mid-range Based Dedicated UNIX Hosting services can be delivered in 60 days. Some environments may take more or less time depending on complexity. Modifications to the agencies existing services are usually are SDC Standard Work.

3.5.7 Service Continuity

For systems within the SDC standard, the system will be restored within 48 hours.

3.5.8 Reporting

Refer to the common section above.

3.5.9 Remedies

Refer to the common section above.

3.6 *Mid-range Based Dedicated i-Series Hosting Service*

Dedicated i-Series Hosting Environment service offering ensures end-to-end delivery of a stable, enterprise hosting environment through the entire lifecycle of the deployment. Disaster recovery systems, which may be requested, are not included by default.

3.6.1 SDC Standard

Mid-range Based i-Series Hosting service offering relate to the specific type of platform. Only two generation of the i-Series operating system on SDC supported hardware are included as part of this service offering.

3.6.2 Scheduled Maintenance

3.6.2.1 Standard Maintenance Window

If maintenance is required, the SDC will use the standard maintenance window. This window will only be used when needed. Use of this window will be governed by the SDC change management process.

Saturday 5pm – 12:00am

3.6.2.2 Patching

High Impact / Pervasive patching (HiPer PTF) is done weekly as needed and Cumulative low impact patching is done quarterly. All patching is scheduled through the Change Management process, but exceptions to the normal schedule can be requested. Emergency critical patches will follow the Urgent or Emergency Change Management process.

3.6.2.3 Privileged Access

Refer to the common section above.

3.6.3 Service Disruption

Refer to the common section above.

3.6.4 Security

Refer to the common section above.

3.6.5 Availability

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

Mid-range Based Dedicated i-Series Hosting services will be available **99.9%** each month.

3.6.6 Request Fulfillment

Most new Mid-range Based Dedicated i-Series Hosting services can be delivered in 60 days. Some environments may take more or less time depending on complexity. Modifications to the agencies existing services are usually are SDC Standard Work.

3.6.7 Service Continuity

For systems within the SDC standard, the system will be restored within 48 hours.

3.6.8 Reporting

Refer to the common section above.

3.6.9 Remedies

Refer to the common section above.

SDC Service Level Agreement

Midrange Hosting Revision History

Date	Author	Description of change
9/28/09	Sean McMullen	Initial draft from internal review.

3.7 zOS Hosting Environment

The SDC offers zOS hosting of your custom or licensed software. These are typically products that serve the customer's mission or business functions. Application code could be produced and maintained by customer staff, on-site contractors, or a contracted vendor.

3.7.1 SDC Standard

The zOS hosting environment service offering refers to the current shared enterprise system hosted on the IBM z-series mainframe. The SDC standard for this environment is an SDC supported zOS version, and various SDC supported utilities. The current list of supported software can be found at: S3 <http://www.oregonsdc.org>. The zOS environment includes all of the major sub-systems and utilities e.g. WebSphere, DB2, CICS, etc., but does not include the zLINUX environment.

3.7.2 Scheduled Maintenance

Refer to the common section above.

3.7.2.1 Standard Maintenance Window

IPL Schedule:

- *1st Sunday each month at 6:30 am*
- *2nd Sunday each month at 6:00pm*
- *3rd Sunday of each month at 4:30 am*

3.7.2.2 Patching

The SDC manages zOS, sub-systems and utility patching. Patching is scheduled through the change management process.

3.7.2.3 Change Management

Refer to the common section above.

3.7.3 Service Disruption

Refer to the common section above.

3.7.3.1 Monitoring

In addition to the basic monitoring, the SDC also monitor the following items for system errors or defined alarm thresholds:

- *Processor*
- *CICS*
- *DB2 Region*
- *Spool Space*
- *Page Space*
- *Disk Pools*
- *IMS Monitoring*

3.7.3.2 Communications / Time to Respond

Refer to the common section above.

3.7.3.3 Time to Restore

Refer to the common section above.

3.7.3.4 Escalations

Refer to the common section above.

3.7.4 Security

Refer to the common section above.

3.7.5 Availability

Availability for the zOS Hosting Environment is limited to the operating system, sub-systems and standard utilities. zOS Hosting availability includes the core network components, but does not include wide-area network components.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

zOS Hosting Environments will be available **99.9%** each month.

3.7.6 Request Fulfillment

New application hosting may be very complex, so please provide as much lead time as possible when planning deployment of new hosted applications. Most major modifications to existing applications can be delivered in 90 days depending on the volume of requests. Some environments may take more or less time depending on complexity.

3.7.7 Service Continuity

Disaster recovery services will be used to restore systems within the SDC standard.

3.7.8 Reporting

Refer to the common section above.

3.7.9 Remedies

Refer to the common section above.

3.8 z/LINUX Hosting Environment

The SDC offers z/LINUX hosting of your custom or licensed software. Application code could be produced and maintained by customer staff, on-site contractors, or a contracted vendor.

3.8.1 SDC Standard

The z/LINUX hosting environment service offering refers to the current shared enterprise system hosted on the IBM z-series mainframe. The SDC standard for this environment is an SDC supported z/LINUX version. The current list of supported software can be found at: S3(
<http://www.oregonsdc.org>.)

3.8.2 Scheduled Maintenance

3.8.2.1 Standard Maintenance Window

IPL Schedule:

- *1st Sunday each month at 6:30 am*
- *2nd Sunday each month at 6:00pm*
- *3rd Sunday of each month at 4:30 am*

3.8.2.2 Patching

The SDC manages z/LINUX patching. Patching is scheduled through the change management process.

3.8.2.3 Change Management

Refer to the common section above.

3.8.3 Service Disruption

Refer to the common section above.

3.8.3.1 Monitoring

In addition to the basic monitoring, the SDC also monitor the following items for system errors or defined alarm thresholds:

- *Processor*

3.8.3.2 Communications / Time to Respond

Refer to the common section above.

3.8.3.3 Time to Restore

Refer to the common section above.

3.8.3.4 Escalations

Refer to the common section above.

3.8.4 Security

Refer to the common section above.

3.8.5 Availability

Availability for the z/LINUX Hosting Environment is limited to the zVM and z/LINUX operating systems. z/LINUX. Hosting availability includes the core network components, but does not include wide-area network components.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

z/LINUX Hosting Environments will be available **99.9%** each month.

3.8.6 Request Fulfillment

New application hosting may be very complex, so please provide as much lead time as possible when planning deployment of new hosted applications. Most major modifications to existing applications can be delivered in 60 days depending on the volume of requests. Some environments may take more or less time depending on complexity.

3.8.7 Service Continuity

Disaster recovery services will be used to restore systems within the SDC standard.

3.8.8 Reporting

Refer to the common section above.

3.8.9 Remedies

Refer to the common section above.

zOS and zLinux Revision History

Date	Author	Description of change
5/20/2009	Sean McMullen	Initial Draft
9/1/2009	Sean McMullen	Changes from zOS internal review.
9/8/2009	Sean McMullen	Changes from zLinux internal review.
10/14/09	Sean McMullen	Format to standard template.
10/29/09	Sean McMullen	Added changes from first External Review Meeting.

3.9 Backup and Restore Services

Backups can be defined as creating a copy of data for purposes of reproducing the original in case the original is lost, erased, damaged, or changed in error. The copy may be an exact duplicate of the original, or it may be some other structure that allows the original to be recreated by restoration software

This SLA sets the expectations on the availability of the systems and software used to backup and restore agency data from systems supported by the SDC. It does not include any guarantee on the quality of the data backed up or on the integrity of the files from those backup. The SDC will ensure that the systems and software used to backup and restore data are functioning properly, but the agency is responsible for testing that the data backed up can be restored.

3.9.1 SDC Standard

The SDC has the following standards for backup and restoration of agency data:

- *Distributed Systems and mid-range based AIX systems use IBM Tivoli Storage Manager (TSM).*
- *Mid-range iSeries systems use IBM Backup Recovery & Media Services (BRMS).*
- *Mainframe systems use the directly attached Virtual Tape System (VTS) and/or Automated Tape Library (ATL).*

3.9.2 Scheduled Maintenance

3.9.2.1 Standard Maintenance Window

If maintenance is required, the SDC will use the standard maintenance window. This window will only be used when needed. Use of this window will be governed by the SDC change management process.

SDC Service Level Agreement

For the TSM server(s):

- *Mon – Thursday 6PM – 10PM,*
- *Sunday 6PM – 12AM*

For the BRMS system:

- *Saturday 5 p.m. to 12 a.m.*

For the ATL and VTS:

- *None (All maintenance is scheduled through the change management process.)*

3.9.2.2 Patching

Patching is as needed. All patching is scheduled through the Change Management process, but exceptions to the normal schedule can be requested. Emergency critical patches will follow the Urgent or Emergency Change Management process.

3.9.2.3 Privileged Access

Due to the shared nature of the environments that host these applications, the SDC cannot grant privileged system access to these environments.

3.9.3 Service Disruption

Refer to the common section above.

3.9.4 Security

Refer to the common section above.

3.9.5 Availability

Service Hours for restorations are 24 x 7 x 365 excluding scheduled maintenance.

Restore Systems will be available **99.9%** each month.

Service Hours for Backup Systems are:

- for TSM 6p.m. – 7a.m. excluding scheduled maintenance
- for BRMS, ATL and/or VTS 24x7x365 excluding scheduled maintenance

Backup Systems will be available **99.9%** each month.

3.9.6 Request Fulfillment

Most backup and restore services for new customers can be delivered in 30 days. Some environments may take more or less time depending on complexity. Modifications to the agencies existing services are usually are SDC Standard Work.

Most agencies have the ability to restore files, but requests for the SDC to restore files are SDC Standard Work.

3.9.7 Service Continuity

For backup systems within the SDC standard, the system will be restored within 96 hours.

3.9.8 Reporting

Refer to the common section above.

3.9.9 Remedies

Refer to the common section above.

Backup and Recovery Revision History

Date	Author	Description of change
9/28/09	Sean McMullen	Initial Draft from internal review.
11/30/09	Sean McMullen	Added changes from first external review.

4 Network and Security

SDC Network and Security Services include the procurement, installation, management, and versioning of hardware and software resources required by customers to connect to and make use of SDC-managed network resources and provide additional confidentiality, integrity and availability of customer data and applications that are hosted by the SDC and are accessed through those network resources.

4.1 Wide Area Network Services (WAN)

The SDC currently offers Wide Area Network (WAN) services throughout the entire state. This service may not be available at certain locations on the state mall is Salem (See State Mall Area Network service). WAN availability varies by area, so the connectivity options may be limited in certain areas. There are two types of WAN services: “on-network” and “off-network”.

- *“On-network” services are those where the SDC provides distribution (DSL modem, router, CSU/DSU, etc.) to the WAN at the local site, transport over a WAN connection (DSL, T-1, DS-3, wireless, fiber, etc.) to the State shared infrastructure, and core services for network traffic across the infrastructure to other networks and the internet.*
- *“Off-network” services are those where the SDC does not provide the core infrastructure. The SDC still provides the distribution, but the WAN vendor provides the central infrastructure and connection to the internet instead of a connection to the State network.*

4.1.1 SDC Standard

SDC Network Standards are detailed in the SDC Architecture document. Hardware that does not conform to these standards will be supported in a reduced capacity.

4.1.2 Scheduled Maintenance

4.1.2.1 Standard Maintenance Window

Sunday 4 a.m. - 6 a.m.

4.1.2.2 Patching

The SDC will perform software updates based upon vendor recommendation regarding Security Vulnerabilities, Network Enhancements and to repair software abnormalities.

4.1.3 Service Disruption

Refer the common section above.

4.1.4 Security

Refer the common section above.

4.1.4.1 Privileged Access

Due to the shared nature of the network environment, the SDC cannot usually grant privileged access to network devices.

4.1.5 Availability

Wide Area Network Services will be available **99.7%** each month.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

4.1.6 Request Fulfillment

Most Wide Area Network services can be delivered in ninety days. Some environments may take more or less time depending on location.

4.1.7 Service Continuity

For systems within the SDC standard, the system will be restored within a maximum of four business days.

4.1.8 Reporting

Refer to the common section above.

4.1.9 Remedies

Refer to the common section above.

4.2 State Mall Area Network

The SDC currently offers network connection services in certain locations on the state mall area in Salem. The mall area network is a high speed loop around selected state office buildings that provides high speed and redundant connections to the state network.

4.2.1 SDC Standard

SDC Network Standards are detailed in the SDC Architecture document. Hardware that does not conform to these standards will be supported in a reduced capacity.

4.2.2 Scheduled Maintenance

Refer to the common section above.

4.2.2.1 Standard Maintenance Window

Sunday 4 a.m. - 6 a.m.

4.2.2.2 Patching

The SDC will perform software updates based upon vendor recommendation regarding Security Vulnerabilities, Network Enhancements and to repair software abnormalities.

4.2.3 Service Disruption

4.2.4 Security

Due to the shared nature of the network environment, the SDC cannot usually grant privileged access to network devices.

4.2.5 Availability

Mall Area Network Services will be available **99.9%** each month.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

4.2.6 Request Fulfillment

Most Mall Area Network services can be delivered in thirty days. Some environments may take more or less time depending on equipment availability.

4.2.7 Service Continuity

For systems within the SDC standard, the system will be restored within a maximum of two business days.

4.2.8 Reporting

Refer to the common section above.

4.2.9 Remedies

Refer to the common section above.

4.3 *Local Area Network Services (LAN)*

LAN connectivity services provide SDC customers with the ability to send and receive data in a secure and reliable manner within their local office.

Physical network elements include switches. Logical network components refer to communications protocols. In the field of telecommunications, a communications protocol is the set of standard rules for data representation, signaling, authentication and error detection required to send information over a communications channel.

The SDC often expands network connectivity offerings by implementing infrastructure to support wireless connectivity in addition to traditional wired networking.

4.3.1 SDC Standard

SDC Network Standards are detailed in the SDC Architecture document. Hardware that does not conform to these standards will be supported in a reduced capacity.

4.3.2 Scheduled Maintenance

Refer to the common section above.

4.3.2.1 Standard Maintenance Window

Sunday 4 a.m. - 6 a.m.

4.3.2.2 Patching

The SDC will perform software updates based upon vendor recommendation regarding Security Vulnerabilities, Network Enhancements and to repair software abnormalities.

4.3.2.3 Change Management

Refer to the common section above.

4.3.3 Service Disruption

Refer to the common section above.

4.3.4 Security

Refer to the common section above.

4.3.4.1 Privileged Access

Due to the shared nature of the network environment, the SDC cannot usually grant privileged access to network devices.

4.3.5 Availability

Local Area Network Services will be available **99.9%** each month.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

4.3.6 Request Fulfillment

Most new and upgraded Local Area Network services can be delivered in thirty days. Some environments may take more or less time depending on equipment availability.

4.3.7 Service Continuity

For systems within the SDC standard, the system will be restored within a maximum of four business days.

4.3.8 Reporting

Refer to the common section above.

4.3.9 Remedies

Refer to the common section above.

4.4 ***Network Support Services – DHCP and/or DNS***

Network Support services provide the SDC customer with the ability to setup their network domains in a secure, manageable, and reliable manner between systems, locations, and users.

Dynamic Host Configuration Protocol (DHCP) provides the automated assignment of Internet Protocol (IP) addresses in a customer's network domain. Using this feature simplifies management of IP addresses when workstations and other addressed devices are moved within the customer's organization.

Domain Name Service (DNS) translates readable text host names into numeric IP addresses. Without this service, network locations must be entered as their numeric address, which is very hard to remember.

4.4.1 SDC Standard

SDC Network Standards are detailed in the SDC Architecture document. Hardware that does not conform to these standards will be supported in a reduced capacity.

4.4.2 Scheduled Maintenance

Refer to the common section above.

4.4.2.1 Standard Maintenance Window

Sunday 4 a.m. - 6 a.m.

4.4.2.2 Patching

The SDC will perform software updates based upon vendor recommendation regarding Security Vulnerabilities, Network Enhancements and to repair software abnormalities.

4.4.2.3 Change Management

Refer to the common section above.

4.4.3 Service Disruption

Refer to the common section above.

4.4.4 Security

Refer to the common section above.

4.4.4.1 Privileged Access

Due to the shared nature of the network environment, the SDC cannot usually grant privileged access to network devices.

4.4.5 Availability

Network DHCP Services will be available **99.9%** each month.

Network DNS Services will be available **99.9%** each month.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

4.4.6 Request Fulfillment

Network support services can be delivered in five business days. Some environments may take more or less time depending on complexity.

4.4.7 Service Continuity

For systems within the SDC standard, the system will be restored within a maximum of two business days.

4.4.8 Reporting

Refer to the common section above.

4.4.9 Remedies

Refer to the common section above.

SDC Service Level Agreement

Network Services Revision History

Date	Author	Description of change
5/20/2009	Sean McMullen	Initial Draft
6/1/2009	Sean McMullen	Completed changes from Management and Team Lead reviews.
9/3/2009	Sean McMullen	Added changes from initial External Review Workgroup
9/4/2009	Sean McMullen	Added changes from second External Review Workgroup

4.5 Remote Access Virtual Private Network (VPN)

A Remote Access VPN instead of using a dedicated, real-world connection such as a leased line, it allows customers the use of a secured "virtual" connection across an untrusted network. Remote Access VPN products provide access to the network domain when the user is at an external location. The remote access VPN provided by the SDC is specifically designed to provide remote network access. It does not provide reverse proxy or application aware services

4.5.1 SDC Standard

Remote VPN access will be provided using a Cisco VPN client or SSL connection from a customer workstation. Workstation support is not provided as part of this service.

4.5.2 Scheduled Maintenance

Refer to the common section above.

4.5.2.1 Standard Maintenance Window

Sunday 4 a.m. - 6 a.m.

4.5.2.2 Patching

Occasionally the SDC will need to patch or upgrade security devices to correct problems or provide new features. When possible, these changes will be implemented taking advantage of the redundant design so that no downtime is seen by the customer. When these changes require downtime, they will be done during the standard SDC maintenance window.

4.5.3 Service Disruption

Refer the common Service Disruption section above.

4.5.4 Security

Refer to the common Security Section Above.

4.5.5 Availability

Remote VPN services will be available **99.9%** each month.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

4.5.6 Request Fulfillment

Most new agency installations of remote access VPN services can be delivered in 60 days. Some changes may take more or less time depending on complexity.

Most minor modifications to the Remote VPN Services are SDC Standard Work.

4.5.7 Service Continuity

For solutions within the SDC standard, the system will be restored within 2 business days.

4.6 Site to Site Virtual Private Network (VPN)

A Site to Site VPN allows the use of a secured "virtual" connection across an un-trusted network. When a site to site VPN is deployed, it encrypts traffic from one network device (such as a firewall or router) to another. Traffic on the local area network is not encrypted.

4.6.1 SDC Standard

Site-to-site VPN is provided only when: 1) an application requires encryption of sensitive data in transit between two sites; and 2) application encryption is unavailable. The SDC Standard is that the SDC will manage the remote encryption device where the remote site is a state agency location.

4.6.2 Scheduled Maintenance

Refer to the common section above.

4.6.2.1 Standard Maintenance Window

Sunday 4 a.m. - 6 a.m.

4.6.2.2 Patching

Occasionally the SDC will need to patch or upgrade security devices to correct problems or provide new features. When possible, these changes will be implemented taking advantage of the redundant design so that no downtime is seen by the customer. When these changes require downtime, they will be done during the standard SDC maintenance window.

4.6.3 Service Disruption

Refer the common Service Disruption section above.

4.6.4 Security

Refer to the common Security Section Above.

4.6.5 Availability

Site to Site VPN Service availability will be part of the WAN availability and available **99.7%** each month.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

4.6.6 Request Fulfillment

Most new site to site VPN services can be delivered in 30 days. Some changes may take more or less time depending on complexity.

4.6.7 Service Continuity

For solutions within the SDC standard, the system will be restored within 48 hours.

4.7 Firewall Management

The SDC firewall service helps prevent unauthorized network access. Firewalls examine network traffic, apply rules definitions, and determine whether data should be forwarded. Firewalls are the first line of defense in protecting information on a network. This service includes:

1. Management of the firewall zones and architecture on the State Wide Area Network.
2. Consultation with customers on protection of their applications and data. Implementation of appropriate firewall rules for customer applications and data protection.
3. Additions, deletions, changes, and management of firewalls, firewall rules, firewall architecture, monitoring, and maintenance.

4.7.1 SDC Standard

SDC Standard is that firewall hardware be located centrally at the data center. Remote firewall hardware may be required but are not within the SDC standard.

4.7.2 Scheduled Maintenance

Refer to the common section above.

4.7.2.1 Standard Maintenance Window

Sunday 4 a.m. - 6 a.m.

4.7.2.2 Patching

Occasionally the SDC will need to patch or upgrade security devices to correct problems or provide new features. When possible, these changes will be implemented taking advantage of the redundant design so that no downtime is seen by the customer. When these changes require downtime, they will be done during the standard SDC maintenance window.

4.7.3 Service Disruption

Refer the common Service Disruption section above.

4.7.4 Security

Refer to the common Security Section Above.

4.7.5 Availability

SDC Firewall hardware will be available **99.9%** each month.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

4.7.6 Request Fulfillment

Most firewall changes can be delivered in one week. Some changes may take more or less time depending on complexity.

Changes requiring additional hardware can be delivered in 30 days. Some changes may take more or less time depending on complexity.

Most firewall changes are SDC Standard Work.

4.7.7 Service Continuity

For systems within the SDC standard, the system will be restored within 48 hours.

Security Services Revision History

Date	Author	Description of change
5/20/2009	Sean McMullen	Initial Draft
6/1/09	Sean McMullen	Completed changes from Management and Team Lead reviews.
6/22/09	Sean McMullen	Changes from SDC Security review.
8/27/09	Sean McMullen	Changes from External Workgroup review.
9/2/09	Sean McMullen	Changes from External Workgroup second review
9/8/09	Sean McMullen	Moved common service levels and appendix into linked documents. (SLA Baseline Common.doc and SLA Baseline Appendix.doc)

4.8 Email Hub Services

An e-mail hub service is a system that sends and receives messages and attached files for multiple e-mail systems. The mail hub system may consist of features such as e-mail firewalling or malware detection and removal.

Agency e-mail applications themselves (server and client) are out-of-scope for the SDC at this time. However, since customer e-mail server applications reside on hardware located at the state data center, physical access restrictions apply.

4.8.1 SDC Standard

The email hub standard is SMTP on port 25.

4.8.2 Scheduled Maintenance

Refer the common section above.

4.8.2.1 Standard Maintenance Window

Sunday 4 a.m. - 6 a.m.

4.8.2.2 Patching

Refer the common section above.

4.8.3 Service Disruption

Refer the common section above.

4.8.4 Security

Refer the common section above.

SDC Service Level Agreement

4.8.4.1 Privileged Access

Due to the shared nature of the environment, the SDC cannot grant privileged access to these devices.

4.8.5 Availability

Email Hub Services will be available **99.9%** each month.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

4.8.6 Request Fulfillment

Most new customers can be delivered mail hub services in two weeks. Some configurations may take more or less time depending on location.

4.8.7 Service Continuity

The mail hub infrastructure is highly redundant but in the unlikely event of multiple hardware failures, the system will be restored within a maximum of 48 hours.

4.8.8 Reporting

Refer to the common section above.

4.8.9 Remedies

Refer to the common section above.

4.9 State E-mail Directory Synchronization

The State E-mail Directory Synchronization provides the agencies a method for maintaining a central state-wide email address list. Agencies identify the addresses that they wish to sync to the state-wide directory, and may setup their systems to sync with the state directory. This synchronization allows agencies to maintain a current state-wide address list for their email clients to use.

This central list also provides the email hub a current list of valid email addresses to help filter out unwanted and invalid email (SPAM).

4.9.1 SDC Standard

Customer systems that conform to the LDAP standards are supported.

4.9.2 Scheduled Maintenance

Refer to the common section above.

4.9.2.1 Standard Maintenance Window

Monday – Friday 1pm – 3pm

4.9.2.2 Patching

Refer to the common section above.

4.9.3 Service Disruption

Refer to the common section above.

4.9.4 Security

Due to the shared nature of the environment, the SDC cannot grant privileged access to these devices.

4.9.5 Availability

State E-mail Directory Synchronization will be available **99.9%** each month.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

4.9.6 Request Fulfillment

Most new customers can be delivered state e-mail directory synchronization services in two weeks. Some configurations may take more or less time depending on location.

4.9.7 Service Continuity

The State E-mail Directory Synchronization infrastructure is redundant but in the unlikely event of multiple hardware failures, the system will be restored within a maximum of 48 hours.

4.9.8 Reporting

Refer to the common section above.

4.9.9 Remedies

Refer to the common section above.

Email Services Revision History

Date	Author	Description of change
11/10/09	Sean McMullen	Initial Draft
11/18/09	Sean McMullen	Added corrections after internal review.
11/30/09	Sean McMullen	Added changed from first external review.

5 Voice

SDC Voice Services include the procurement, installation, management, and versioning of hardware and software resources required by customers to connect to and use voice telecommunications through SDC-managed resources. Cellular voice communications are excluded.

Voice Services provides telephone communications over traditional lines or by Voice over Internet Protocol (VOIP). Voice Services provides voice technologies for state agencies throughout Oregon. It is their goal to provide accurate, reliable sustainable technologies, contracts, and information that are sound from a budgetary standpoint as well as a technological and architectural perspective.

SDC Voice Services takes an oversight role in all state agency voice projects, assisting, educating, and coordinating customers and vendors through necessary processes and procedures. SDC's role ensures that all associated state standards, contracts, statutes and administrative rules are adhered to for risk mitigation and assurance of a quality project result.

ORS 283.140 defines Voice Services roll as follows:

SDC Service Level Agreement

“The Oregon Department of Administrative Services shall exercise budgetary management, supervision and control over all telephone and telecommunications service for all state agencies...”

5.1 Traditional Phone Systems

Depending on business requirements, agencies are provided with local premise based equipment that provides access to State voice network vendor provided facilities. If required, locations can be provided redundant capabilities to further protect the location from loss of service. Users are also provided with an array of electronic telephone instruments to choose from to meet their specific business needs. Voice mail, long distance call detail reporting, maintenance, and software changes, are included in the service.

5.1.1 SDC Standard

The standards for Traditional Phone Systems are those using SDC standard equipment. Excluded are those systems not on the state network. (Off-net)

5.1.2 Scheduled Maintenance

5.1.2.1 Standard Maintenance Window

Central Office Maintenance Window – 10:00pm – 6:00am

5.1.2.2 Patching

Patching, if required, will be scheduled through SDC Change Management.

5.1.3 Service Disruption

5.1.3.1 Monitoring

Individual key systems and PBXs on the state system are not monitored for up/down state, but the trunking to the systems is monitored by SDC vendors.

5.1.3.2 Communications / Time to Respond

On all outages an initial status of Service-affecting troubles will be available within 30 minutes of the initial report.

5.1.3.3 Time to Restore

- *Within 1 business day for minor outages*
- *Within 8 hours for major outages*
- *Within 4 hours for critical outages.*

For all outages expected to take more than 4 hours to resolve, Contractor shall provide an "ETTR" (or estimated time to repair) within 45 minutes.

-

*A **critical** outage is defined as one that disrupts Service to more than 25% of users, or 10 users, whichever is fewer, at any one location at any one time. A **major** outage is one that disrupts Service to less than 25% of users, or 10 users, whichever is fewer, but more than 5% of users, or 2 users, whichever is fewer, in any one location at any one time. A **minor** outage is one that disrupts Service to less than 5% of users, or two users, whichever is fewer, in any one location at any one time. In addition to these conditions, the State reserves the right to define outage criteria in accordance with the State's unique operational needs.

5.1.4 Security

This section replaces and supersedes the common Security section above.

The SDC contracts with its long distance provider to monitor and detect unusual calling activity and fraudulent calls. This form of network insurance covers long distance, calling cards and usage patterns.

5.1.4.1 Intrusion Detection

Toll fraud prevention measures shall include, by way of example, but not as a complete list, the following by SDC or its contractors:

- *Ensuring that callers cannot transfer to an outside trunk through voice mail, automated attendant, IVR, and other attachments.*
- *Ensuring that all default passwords are changed upon installation.*
- *Ensuring that maintenance ports are adequately secured with passwords that are non-trivial and changed monthly, or immediately upon knowledge of incident in the event of a security breach.*
- *Ensuring that vulnerable ports such as DISA (Direct Inward System Access) are deactivated and remain so.*
- *Ensuring that restrictions and class of service are designed and administered to narrowly restrict access to vulnerable features such as off-system forwarding and trunk access codes.*
- *Ensuring that calls are blocked to overseas locations and the Caribbean area codes except for those classes of service that must have access to them. (Requires letter from agency director accepting fraud risk).*
- *SDCs contractor will telephonically notify the NCC immediately upon any discovery of potential toll fraud.*

5.1.4.2 Security Incident Response

The SDC will notify ESO and agency security personnel of intrusion incidents and suspicious activities in accordance with the SDC and agency Security Incident Response Plan. The agency must designate who will receive these types of notifications.

5.1.5 Availability

Traditional Phone services (PBX and Key Systems) will be available **99.9%** each month.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

5.1.6 Request Fulfillment

New phone systems vary in complexity so contact the SDC as early as possible when ordering.

Move, Add, Change and Disconnect Support and Order Intervals

SDC and its contractor shall complete State approved TSOs according to the guidelines listed below. Complete at least 95% of all service orders within three working days of receipt. Detailed requirements are as follows:

- a. TSOs affecting 1-20 stations shall be completed within three working days.
- b. TSOs affecting 21-50 stations shall be completed within five working days.
- c. TSOs affecting more than 50 stations shall be completed as agreed on an individual case basis.
- d. Complex Service TSOs involving MACD, IVR, ACD or any related Call Center Services shall be completed on an individual case basis (ICB).

SDC Service Level Agreement

Individual Case Basis (ICB) commitments shall be negotiated during planning/forecasting sessions in which the State, user representatives and Contractor's personnel may participate.

5.1.7 Service Continuity

For solutions within the SDC standard, the system will be restored under the Service Disruption standards.

5.2 Voice Over IP (VOIP) Phone Systems

VOIP enables voice conversations to be sent over customer LANs, the SDC WAN, and the Internet. Voice mail, caller ID, call forwarding and other usual and customary services associated with traditional phone service are typically part of a VOIP package. Additional services that may be available include softphones (i.e., a software-based phone that requires using the computer to make and receive calls) and unified messaging, which allow users to receive and access voice-mail messages through their e-mail client.

5.2.1 SDC Standard

SDC VOIP Standards are detailed in the SDC Architecture document. Hardware that does not conform to these standards will not be supported.

5.2.2 Scheduled Maintenance

5.2.2.1 Standard Maintenance Window

Sunday 4 a.m. - 6 a.m.

5.2.2.2 Patching

All servers are patched and upgraded according to the manufacturer's recommendations.

5.2.3 Service Disruption

Refer the common Service Disruption section above.

5.2.4 Security

Refer to the common Security Section Above.

5.2.5 Availability

VOIP services will be available **99.9%** each month.

Service Hours are 24 x 7 x 365 excluding scheduled maintenance.

5.2.6 Request Fulfillment

New VOIP phone systems vary in complexity so contact the SDC as early as possible when ordering.

<u>Description</u>	<u>Process</u>	<u>Timeline</u>
MACD (Move/Add/Change/Delete) Activity: <ul style="list-style-type: none">➤ Add a mailbox➤ Delete a mailbox➤ Change mailbox name➤ Change zero out	Email to VoIPChange@das.state.or.us	4-6 hours

SDC Service Level Agreement

<ul style="list-style-type: none"> ➤ Change/reset mailbox password ➤ Change mailbox characteristics (msg envelope) ➤ System deletion of messages ➤ Change name on phone ➤ Change phone capabilities (FWD BSY/NA, HF answer, Pick up group, page zone, etc.) ➤ Change what lines appear/ring ➤ Add/delete/edit speed dials ➤ Add/delete/edit/apply line restrictions 		
Advanced Vmail/ACD Activity: <ul style="list-style-type: none"> ➤ Add/delete/edit voice menu ➤ Auto attendant programming ➤ CCR Tree programming ➤ Add new IPCC (ACD) agent 	TSO	3-5 days
Install/Disconnect Activity: <ul style="list-style-type: none"> ➤ Install a new phone ➤ Remote/Disconnect a phone and return phone to warehouse ➤ Move a phone to a new building 	TSO	3-5 days
Move a phone inside current building	User can complete	NA

5.2.7 Service Continuity

For solutions within the SDC standard, the system will be restored within 48 hours.

Security Services Revision History

Date	Author	Description of change
9/14/2009	Sean McMullen	Initial Draft
9/21/09	Sean McMullen	Changes from External Workgroup review.

6 Appendix

6.1 Definitions

6.1.1 Automated Call Distributor

A computerized phone system that responds to the caller with a voice menu and connects the call to the appropriate agent. It can also distribute calls equally to agents. ACDs are the heart of call centers, or contact centers, which are widely used in the telephone sales and service departments of all organizations.

6.1.2 Availability:

Ability of a component or service to perform its required function at a stated instant or over a stated period of time. It is usually expressed as the availability ratio, i.e. the proportion of time that the service is actually available for use by the Customers within the agreed service hours. In the Service Level Agreement the availability percentages are derived using the following formula:

$$[(\text{THS} - \text{DT}) / \text{THS}] \times 100 = \text{Service or Component Availability (\%)}$$

THS = Total Hours of Service

DT = Actual downtime during agreed service time

6.1.3 Best Effort

Best effort support defines SDC support levels for non-standard software and hardware. There are no service guarantees for non-standard hardware and software. In general the SDC will provide professional services to the extent possible. Best Effort however assumes that the level of support offered for these systems is something less than what is guaranteed for standard systems.

6.1.4 Catastrophic Failure:

A catastrophic failure is a sudden and total failure of some system from which recovery is impossible.

6.1.5 Change Management:

The SDC Change Management process provides communication and control over the addition, modification or removal of hardware and software that could have an effect on IT services. The change management process includes both an SDC internal and customer-inclusive review of change requests. For customer agencies that have their own internal change management process, the SDC Change Manager will work with the agency Change Manager to integrate processes to meet both SDC and customer needs.

6.1.6 Custom Call Routing (CCR) Tree

A Custom Call Routing (CCR) Tree contains paths that callers select using their touch-tone phones. They are prompted by a series of recordings. Once a selection is made, they are routed to messages, transferred to extensions or departments, or directed to sub menus for more specific information.

6.1.7 Customer:

In the SDC Service Level Agreement, the term "Customer" refers to state agencies or other public organizations that request and acquire services provided by the SDC.

6.1.8 Delivery Date:

The date that the service is available for the customer to use. This is typically at the end of the Solutions Release phase of the SDC Engineering workflow.

6.1.9 Down Time (DT):

The amount of time between when the SDC was notified that a service became unavailable, and when service was restored. Notification can come from either the SDC monitoring system, or the customer. Down Time excludes planned maintenance and service disruptions caused by factors beyond the SDC control (remote power outages, application changes applied by the customer, etc.)

6.1.10 Expected Delivery Date:

The date that the service is expected to be delivered. Customers are provided an Expected Delivery Date once the requirements are determined and the solution design developed. This typically occurs at the end of the Plan Development phase of the SDC Engineering workflow.

6.1.11 Forward Busy (FWD-BSY)

Incoming calls go directly to voice mail if line is busy.

6.1.12 Forward No Answer (FWD-NA)

Incoming calls go to voice mail after 3 or 4 rings

6.1.13 Hands Free (HF) Answer

The ability to answer calls without picking up the handset.

6.1.14 Hours of Service:

The number of hours per day and the number and which days of the week that support will be provided for a given Service Level. (e.g. 24x7, 12x5, etc.)

6.1.15 Interactive Voice Response (IVR)

An automated telephone information system that speaks to the caller with a combination of fixed voice menus and data extracted from databases in real time. The caller responds by pressing digits on the telephone or speaking words or short phrases. Applications include bank-by-phone, flight-scheduling information and automated order entry and tracking.

6.1.16 Internet Protocol Contact Center (IPCC)

A Cisco product to provide Automated Call Distribution (ACD) and other enhanced features for voice over internet protocol (VOIP).

6.1.17 Key System (Voice)

An in-house telephone system that is not centrally connected to a PBX. Also known as a "key system," each telephone has buttons for outside lines that can be dialed directly without having to "dial 9."

6.1.18 Private Branch eXchange (PBX)

An in-house telephone switching system that interconnects telephone extensions to each other as well as to the outside telephone network (PSTN). A PBX enables a single-line telephone set to gain access to one of a group of pooled (shared) trunks by dialing an 8 or 9 prefix. PBXs also include functions such as least cost routing for outside calls, call forwarding, conference calling and call accounting. Modern PBXs use all-digital methods for switching, but may support both analog and digital telephones and telephone lines.

6.1.19 Privileged Access:

Access that allows an individual access to SDC computer, network, or security resources when that access provides the capability to alter the properties, behavior or control of the information system or network.. Privileged access is typically granted to system administrators, network administrators or other such employees whose job duties require such access.

6.1.20 Public Switched Telephone Network (PSTN)

The worldwide voice telephone network. Also called the "plain old telephone system" (POTS) and originally analog only, the heart of most telephone networks today is digital. However, the lines from the home and office to the digital loop carrier (DLC) junction box in the neighborhood typically remain analog. At that point, analog signals are converted to digital.

6.1.21 Service:

The deliverables of the IT organization as perceived by the Customers. Contains one or more IT systems working together to enable a business process.

6.1.22 SDC Engineering Request

New, modified, or enhanced services or support that requires consulting, exploration of options, customer submission of requirements, agreement by SDC (and customer of SDC) for those requirements, funding approval, and appropriate change management. If a request is one of an agencies top eight priorities, it is processed as an Engineering Work Required request regardless of its duration or change management impact.

6.1.23 SDC Standard Work

Work that has been proven possible to complete in 0 - 6 hours that has received standing approval through change management, or work that does not need to go through the change management process.

6.1.24 Service Disruption:

Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service.

6.1.25 Severity Level:

An assessment of the degree of impact a Service Disruption has on the end-user that is used to prioritize response to reported outages.

(See http://www.oregon.gov/DAS/SDC/docs/Service_Catalog.pdf Appendix A for details)

6.1.26 Service Level:

The agreed upon level of quality for a service. (e.g. Availability, Time to Respond, Time to Restore, etc.)

6.1.27 Service Level Measurement:

The measurement of the service level that describes the quality of the service for a period of time. (e.g. the Wide-Area Network (WAN) availability for July, 2008 was 99.98%)

6.1.28 Time to Respond:

The amount of time available for a response to an incident from the appropriate SDC support personnel. This is the time for triage on the Incident to begin at a minimum.

6.1.29 Time to Restore:

The amount of time that is taken to return a given service to normal levels of performance from the onset of an Incident to the point where adequate checks have taken place to ensure that the service has been restored..

6.1.30 Total Hours of Service (THS):

The total number of hours within a given period that a service was expected to be available. (e.g. For the month of January for a 24x7 service with 3hrs of maintenance window: $31 \times 24 - 3 = 741$ hrs)

6.1.31 Untrusted Network:

Any network where physical and/or logical access are not subject to monitoring, administration and supervision of the SDC.

Appendix Revision History

Date	Author	Description of change
9/8/2009	Sean McMullen	Initial Draft
9/21/09	Sean McMullen	Added definitions from Voice External Workgroup.