



Oregon State Data Center

Architecture Request for Proposals (RFP) Guidelines

SDC Customer Requests SDC customers issuing RFPs to support application development initiatives often have hardware requirements. Standards and guidelines for equipment housed at the SDC are outlined below.

SDC Responsibility: SDC is charged with providing hardware and software solutions that can be efficiently maintained and supported. New agency or statewide projects should integrate into the environment and support mechanisms that SDC provides so the highest possible savings is realized.

Solutions that are outside the State's consolidation efforts (e.g., third-party, vendor supported hardware and software) are not within SDC scope. With regard to hardware and licensed software (for new projects), SDC:

- Obtains the hardware needed to support the vendor proposed solution. This requires SDC to work with the agency to obtain the correct specifications as to appropriately scale the needed hardware. Likewise, SDC acquires and installs licensed software platforms (i.e. WebSphere, .NET, etc.). SDC and agency coordinates on the correct configuration(s) of these licensed software platforms.
- Works through its contracted hardware and software providers to obtain (and pay for) the needed software and licenses required to support the vendor proposed solution.
- Establishes agreements, in conjunction with SDC contracted hardware and software providers, addressing State required warranties and warranty periods. This agreement is between the State and State contracted hardware and software provider.

Vendor Responsibility: Vendors are encouraged to propose solutions which are compatible with the Oregon State Data Center (SDC) IT infrastructure standards.

Assumptions: Vendors are expected to consider general SDC standards and conditions below:

1. Software Solutions: The solution architecture software:

- A. The software environment (language) should be 'open' or built upon 'industry standards' (e.g. WebSphere, Java, .NET, PHP, etc.)
- B. The software solution should run on open or 'industry standard' operating systems (e.g. AIX, Windows, Z/OS, Linux)

2. Hardware/OS Platform Solutions: SDC uses the hardware/OS Platform Standards below:

- A. pSeries: The SDC runs UNIX applications on IBM pSeries AIX
- B. zSeries: State zSeries mainframes run applications under Z/OS v1.9 (currently 1.7 but will soon be 1.9)
- C. iSeries: State iSeries mainframes run applications under i5OS
- D. Linux solutions runs on Intel based hardware or on zSeries mainframe; SDC standard O/S for Linux solutions is SuSE.

3. Intel-Based Hardware Solutions: SDC uses the hardware/OS Platform Solutions below:

- A. Standard for deployment into Intel-based environments is to use virtualization technologies (VMWare ESX) whenever possible. The platform selection is structured as follows:
 - 1. use of a virtual server will be explored first; if not viable, then
 - 2. use of a blade server; if not viable then the last option will be
 - 3. use of a stand alone server
- B. Standardized on HP DL Series hardware. Any hardware brought into the SDC through this RFP process is configured to SDC standard or, at minimum, has the configuration quality assurance reviewed by the SDC.
- C. Windows Server 2008 r1 and 2003 (32-bit and 64-bit) Standard and Enterprise Operating Systems and SuSE Linux Enterprise Server

4. Backup Solutions: SDC uses the Backup Solutions Standards below:

- A. Backups are made for all open systems platforms using IBM Tivoli Storage Manager (TSM)
- B. Backups are performed by the SDC and incorporate the Automated Tape Library
- C. Backups of DB's will utilize the Tivoli Data Protection agent

5. Database Management Solutions: SDC supports Data Base Mgmt Systems (DBMS) below:

- A. DB2 on Z/OS mainframe, iSeries mainframe and pSeries AIX
- B. Microsoft 2008 SQL Server for MS Windows 2003
- C. ORACLE v11 on pSeries AIX
- D. MySQL on Linux and MS Windows

6. Storage Solutions: All platforms use Hitachi SAN and ATL for data storage. SDC provides a tiered storage environment to its customers with the ability to use and allocate the appropriate storage type based on predetermined business classification and requirements. Storage tiers are created to support different I/O workloads. The tiers and their purposes:

- A. **Tier 1 (Disk):** Highest availability with fastest performance (mainframe and databases). Suitable for high availability applications with high I/O.
- B. **Tier 2 (Disk):** High availability with fast performance (databases/file servers)
- C. **Tier 3 (Disk):** high availability with average performance (file servers, images and backup/archive). Not suited for high random I/O.
- D. **Tier 4 (Tape):** Moderate availability with average performance (backup/archive)
- E. **Offsite Storage:** Available within hours or days (archive/disaster recovery)

7. Network Solutions:

- A. SDC typically uses a frame relay (1.024Mbps) network, Ethernet (2Mbps – 10Mbps) and a direct digital (1.544Mbps) network. Some sites may have bandwidth as low as 56Kb. SDC uses MPLS VPN services to isolate agency networks on a shared infrastructure.
- B. Standard protocols for SDC networks:
 - 1. IPv4/IPv6 (in development)
 - 2. Ethernet (10/100 Mbps) is available for LANs
 - 3. Ethernet (1000 Mbps) is available for servers

8. Security:

- A. SDC is currently not PCI compliant and does not have plans to become compliant.
- B. The SDC is not currently configured for collocation standards.
- C. The SDC will manage internal firewall configurations.
- D. SDC VPN includes the procurement, installation, management, and versioning of hardware and software resources required by customers to connect to and make use of SDC-managed VPN resources.

9. General Comments:

- A. If business requirements include encryption of data, SDC prefers the encryption to be at the application level to cause the least disruption to infrastructure support.
- B. Prior to implementation in SDC's production environment, new products should be installed in the SDC test environment and reviewed for system performance and consistency with SDC environments. Products found to be incompatible with the SDC environment will be modified as needed.
- C. Software and applications shall use system standard protocols for security authentication (i.e., active directory for Windows, RACF for z/OS, eDirectory for Novell Servers, LDAP) rather than internal security methods.
- D. The SDC will provide and support all services using a set of service management standards and processes based on the activities identified in the IT Infrastructure Library (ITIL) v3 Service Lifecycle. SDC staff, management, and contractors will adhere to the SDC's documented standards and processes.
- E. Implementation planning should include an SDC operations visit to discuss questions; e.g., :
 - What is the business criticality of this application?
 - What process should be used to engage agency resources for production issues during business hours?
 - What are the normal business hours for this application?
 - Are there specific agency contacts that should be notified in case of an after-hours emergency?
 - Are there special "seasons" of increased activity for this application where up-time is critical to the business?

Rates/charges: <http://oregon.gov/DAS/SDC/rates.shtml>

SDC Service Catalog: <http://oregon.gov/DAS/SDC/services.shtml>

SDC Facility Information: In 2005, Oregon state government finished building a new data center to serve the majority of the state's computing needs. The design of the facility and its infrastructure meets the Uptime Institute's standards for Tier III certification 99.9% uptime. The institute's classification system creates a benchmark for reliable infrastructure design in data centers. Achieving Tier III standards means the State Data Center's facility is a vast improvement over the state's previous data centers.

For more information: Contact: servicedesk@das.state.or.us (request to be logged and tracked; questions will be directly coordinated with appropriate subject matter expert).