

# Enterprise Information Services Data Center Services Service Catalog



*Ensuring accessible, reliable and secure state technology systems that serve Oregonians.*

January 2023

**Contents**

- DCS Services .....3
- Local Area Network .....6
- State Network Access.....8
- Backup.....10
- Data Storage.....12
- IT Professional Services .....14
- Colocation.....16
- Hosting .....18
- Cloud Services .....21
- Appendix A .....24
- 3.1 Linux .....25
- 3.2 Windows .....27
- 3.3 Disaster Recovery/System Recovery .....29
- 3.4 Active Directory.....29
- 3.5 File and System Backup .....30
- 3.6 DNS .....30
- 3.7 Mainframe.....31
- 3.8 iSeries .....32
- 3.9 UNIX .....34
- 3.10 Network.....36
- 3.11 Colocation .....37
- 3.12 Privileged Access .....37
- 3.13 General Support .....38

This catalog provides an overview to help customers select managed IT services provided by Data Center Services (DCS).

As a DCS customer, a dedicated Account Manager is assigned to your agency. Your Account Manager is the primary contact for your executive management, assists with planning, and helps you select services to address your business objectives. Your Account Manager is your primary point of contact with DCS.

**How to get started with a new service?** For new customers, contact an Account Manager by calling 503-378-6758 or email [DCS.Info@das.oregon.gov](mailto:DCS.Info@das.oregon.gov). Existing customers can enter a service request through our service management system [IVANTI](#).

# DCS Services

Service	Summary	Page
<b>Data Network Services</b>		
Local Area Network	Local area network services provide networking of computing devices within the customers' physical locations and to the state network, allowing: <ul style="list-style-type: none"> <li>• Computing resources such as files, printers, and applications to be shared.</li> <li>• Data and messages to be sent and received in a secure and reliable manner.</li> </ul>	<b>6</b>
State Network Access	State network access services provide connectivity to state and agency resources (such as servers at DCS), to other governmental offices that are connected to the state network, and to the Internet.	<b>8</b>
<b>Data Storage Services</b>		
Backup	Backup services create reliable copies of data, related software and supporting configurations for the purpose of reproducing data from a specific point in time in the event the original is lost, erased, damaged, or changed in error.	<b>10</b>
Data Storage	Data storage services provide secure technology and capacity management to store customers' data in a manner that meets their performance and availability needs.	<b>12</b>
<b>IT Professional Services</b>		
IT Professional Services	IT professional services provide general technical support and consulting to meet customer short-term technology needs.	<b>14</b>
<b>Managed Computing Services</b>		
Colocation	Colocation services provide customers the ability to host their IT equipment in the state's Data Center, taking advantage of the tier 3 infrastructure, leveraging economies of scale, and reducing the expense of maintaining datacenters for customer-owned systems.  DCS provides the physical building, cooling, power, fire protection, surveillance, N+1 resiliency of a tier 3 datacenter and 24/7 unescorted access.	<b>16</b>

<p>Hosting</p>	<p>DCS engineers, builds, and supports customized hosting solutions designed to help customers improve IT quality, efficiency, and reliability. Depending on infrastructure needs, DCS can virtualize existing servers, build an entire custom hosted infrastructure, or simply provide a managed server. DCS' wide array of professional capabilities to provide the right solution to meet customers' needs.</p>	<p><b>18</b></p>
<p>Cloud</p>	<p>DCS enables agency IT divisions, developers, and end-users to quickly access and deploy cloud environments with minimal friction and IT overhead while maintaining effective guardrails through centralized policies and procedures that leverage pre-built templates.</p> <p>DCS has options tailored to accommodate distinct needs:</p> <ul style="list-style-type: none"> <li>• Native Cloud Offering – Core Enterprise Organization Cloud Framework with security services and available private transit to State of Oregon network</li> <li>• EIS-Managed Cloud Offering – Native Cloud Offering plus DCS Compute services within the cloud environment</li> </ul>	<p><b>21</b></p>

# Local Area Network

## 1. What is the service?

<p>a. Service Summary</p>	<p>Local area network services provide networking of computing devices within the customers' physical locations and to the state network, allowing:</p> <ul style="list-style-type: none"> <li>• Computing resources such as files, printers, and applications to be shared.</li> <li>• Data and messages to be sent and received in a secure and reliable manner.</li> </ul>
<p>b. Description of the features and benefits of the service</p>	<p>LAN services provide the staff and expertise to manage the customer's internal network, networking equipment such as switches and wireless access points required to provision the LAN, and all the communications protocols needed for the exchange of data and messages.</p>
<p>c. Offerings and options</p>	<p>This service can be provided in two different ways:</p> <ol style="list-style-type: none"> <li>1. Wired LAN: Devices physically connected to the LAN with cables. Wired LANs require the use of central devices like switches, offer high reliability, and superior performance.</li> <li>2. Wireless LAN: Devices connected to the LAN without cables. Wireless LANs, sometimes referred to as WLANs, are provided through Wi-Fi signals. They are less reliable than wired LANs and have more limited performance capability but offer greater mobility.</li> </ol> <p>Options:</p> <ol style="list-style-type: none"> <li>1. Customers may also opt to have secure user remote access (end user VPN) to allow individuals to access specified computer resources through the Internet.</li> <li>2. The service provides IP addresses for devices to be connected to the LAN. Customers may choose to manage IP addresses themselves or have DCS manage them.</li> </ol>
<p>d. Service prerequisites</p>	<p>State Network Access service</p>
<p>e. Description of what is not included in the service</p>	<p>Wiring, HVAC, power, and backup power at the customer's location is to be provided by the customer. DCS can assist with contracting for required wiring if necessary.</p>

## 2. How is the service requested?

a. Service request options:	Services are requested through IVANTI, the DCS secure on-line support system, at <a href="https://oregondcsesm-amc.ivantcloud.com/">https://oregondcsesm-amc.ivantcloud.com/</a> . New customers may Contact an Account Manager @ 503-378-6758 or email <a href="mailto:DCS.Info@das.oregon.gov">DCS.Info@das.oregon.gov</a>
b. What forms are used/needed to request this service?	Online general request form on IVANTI.
c. When can you expect to have your service request fulfilled?	Most services can be delivered within thirty days. Some environments may take more or less time depending on location.
<b>3. How do I get help? How does the program/Service Enterprise provide support to customers of this service?</b>	
a. Self-service support	There is currently no self-service support for this service.
b. Requesting support	<p>If experiencing a disruption of service or severe degradation of service, call 503- 373-1000 (DCS Service Desk) or Submit an Incident through IVANTI.</p> <p>For changes or modifications to the service, use the general request process through IVANTI.</p>
c. When can you expect to get a response?	<p>DCS follows standardized response times for all services. Customers should expect DCS staff to respond within the following time frames:</p> <ul style="list-style-type: none"> <li>Severity 1 service disruptions – 15 minutes</li> <li>Severity 2 service disruptions – 60 minutes</li> <li>Severity 3 service disruptions – 1 business day</li> <li>Severity 4 service disruptions – 2 business days</li> <li>Requests for changes or modifications– 3 business days</li> </ul> <p>Severity levels for service disruptions are determined by the scope and impact of the individual incident. See incident response section of SLA for description of severity levels.</p>

# State Network Access

1. What is the service?	
a. Service Summary	State network access services provide connectivity to state and agency resources (such as servers at DCS), to other governmental offices that are connected to the state network, and to the Internet.
b. Description of the features and benefits of the service	<p>State network access provides:</p> <ol style="list-style-type: none"> <li>1. A redundant core infrastructure.</li> <li>2. Bandwidth to the state network.</li> <li>3. Segregated customer network environments.</li> <li>4. Allocated IP address blocks.</li> <li>5. Intrusion detection and monitoring.</li> <li>6. Internet connectivity.</li> <li>7. Tools for customers to use to monitor their agency's network traffic.</li> </ol>
c. Offerings and options	<p>The customer has a broad range of options for bandwidth connecting to the state network. That bandwidth will be dictated by the location of the remote site and various other factors including equipment availability and wiring at the site.</p> <p>Options: customer may choose the following additional functionality:</p> <ol style="list-style-type: none"> <li>1. Site-to-site private networking to allow network traffic to be encrypted across the network between two sites.</li> <li>2. Secure, High availability using Software Designed Wide Area Networks (or SD-WAN), redundant circuits and redundant equipment for critical sites.</li> <li>3. Secure user remote access (end-user VPN) allowing an individual to access specified computer resources through the Internet.</li> </ol>
d. Service prerequisites	<p>Connection from the public switched network to the customer's on-site wiring. This is usually provided by the site owner through a conduit from a point near the property border to a network interface device in the building, commonly called the "demarc" or demarcation point.</p> <p>DCS can assist with contracting for establishing the conduit and interface if required.</p>
e. Description of what is not included in the service	Wiring, HVAC, power, and backup power at the customer's location is to be provided by the customer. DCS can assist with contracting for required wiring if necessary.



<b>2. How is the service requested?</b>	
a. Service request options:	Services are requested through IVANTI, the DCS secure on-line support system, at <a href="https://oregondcsesm-amc.ivantcloud.com">https://oregondcsesm-amc.ivantcloud.com</a> . New customers may Contact an Account Manager @ 503-378-6758 or email <a href="mailto:DCS.Info@das.oregon.gov">DCS.Info@das.oregon.gov</a> .
b. What forms are used/needed to request this service?	Online general request form on IVANTI.
c. When can you expect to have your service request fulfilled?	Most services can be delivered within ninety days. Some environments may take more or less time depending on location.
<b>3. How do I get help? How does the program/Service Enterprise provide support to customers of this service?</b>	
a. Self-service support	Network traffic monitoring through tools provided by DCS at the request of the customer.
b. Requesting support	<p>If experiencing a disruption of service or severe degradation of service, call 503- 373-1000 (DCS Service Desk) or Submit an Incident through IVANTI.</p> <p>For changes or modifications to the service, use the general request process through IVANTI.</p>
c. When can you expect to get a response?	<p>DCS follows standardized response times for all services. Customers should expect DCS staff to respond within the following time frames:</p> <ul style="list-style-type: none"> <li>Severity 1 service disruptions – 15 minutes</li> <li>Severity 2 service disruptions – 60 minutes</li> <li>Severity 3 service disruptions – 1 business day</li> <li>Severity 4 service disruptions – 2 business days</li> <li>Requests for changes or modifications– 3 business days</li> </ul> <p>Severity levels for service disruptions are determined by the scope and impact of the individual incident. See incident response section of SLA for description of severity levels.</p>

# Backup

1. What is the service?	
a. Service Summary	Backup services create reliable copies of data, related software and supporting configurations for the purpose of reproducing data from a specific point in time in the event the original is lost, erased, damaged, or changed in error.
b. Description of the features and benefits of the service	<p>The base service includes:</p> <ol style="list-style-type: none"> <li>1. A primary backup copy at the state's Data Center.</li> <li>2. A secondary backup copy generated and stored offsite.</li> <li>3. Creation of full backups which provide complete copies of the content of the selected file.</li> <li>4. Creation of incremental backups which only copies the content of the designated files that have been changed since the last full backup, making backup sizes, and run times more economical and efficient.</li> <li>5. Tools for customers to monitor usage and to restore backups.</li> </ol>
c. Offerings and options	Customers define their backup requirements and are given the tools to restore their data. Additional assistance from DCS is available for data restoration.
d. Service prerequisites	Hosting service or state network access.
e. Description of what is not included in the service	<p>This service does not provide:</p> <ol style="list-style-type: none"> <li>1. Data archiving. Data archiving is used for long-term retention of inactive data that must be maintained for regulatory compliance and includes indexing and search capabilities. The backup service is intended to be used to restore corrupted or destroyed data only.</li> <li>2. Disaster recovery of the hosting server environment. If the data being backed up is from systems or applications hosted by DCS, this function may be provided as an option under that service.</li> </ol>
2. How is the service requested?	
a. Service request options:	Services are requested through IVANTI, the DCS secure on-line support system, at <a href="https://oregondcsesm-amc.ivanticloud.com">https://oregondcsesm-amc.ivanticloud.com</a> . New customers may Contact an Account Manager @ 503-378-6758 or email <a href="mailto:DCS.Info@das.oregon.gov">DCS.Info@das.oregon.gov</a>

b. What forms are used/needed to request this service?	Online general request form on IVANTI.
c. When can you expect to have your service request fulfilled?	Most backup services can be delivered within 30 days. Some environments may take more or less time depending on complexity.
<b>3. How do I get help? How does the program/Service Enterprise provide support to customers of this service?</b>	
a. Self-service support	<p>Monitoring of backups - Backups can be monitored in two ways:</p> <ol style="list-style-type: none"> <li>1. An auto generated report of backup activity distributed to emails the customer has identified.</li> <li>2. Graphical interface provided when backup service is established.</li> </ol>
	Backup restoration – Backup restorations are performed using the same graphical interface as used for monitoring.
b. Requesting support	<p>If experiencing a disruption of service or severe degradation of service, call 503- 373-1000 (DCS Service Desk) or Submit an Incident through IVANTI</p> <p>For changes or modifications to the service, use the general request process through IVANTI.</p>
c. When can you expect to get a response?	<p>DCS follows standardized response times for all services. Customers should expect DCS staff to respond within the following time frames:</p> <ul style="list-style-type: none"> <li>Severity 1 service disruptions – 15 minutes</li> <li>Severity 2 service disruptions – 60 minutes</li> <li>Severity 3 service disruptions – 1 business day</li> <li>Severity 4 service disruptions – 2 business days</li> <li>Requests for changes or modifications– 3 business days</li> </ul> <p>Severity levels for service disruptions are determined by the scope and impact of the individual incident. See incident response section of SLA for description of severity levels.</p>

# Data Storage

## 1. What is the service?

a. Service Summary	Data storage services provide secure technology and capacity management to store customers' data in a manner that meets their performance and availability needs.
b. Description of the features and benefits of the service	<p>The base service includes:</p> <ol style="list-style-type: none"> <li>1. Reserved storage space.</li> <li>2. Capacity increase/decrease upon request.</li> <li>3. Usage reporting.</li> <li>4. Customer controlled retention.</li> <li>5. Storage infrastructure management</li> </ol>
c. Offerings and options	<p>Storage tiers enable customers to determine which level of storage performance best meets their price and availability requirements. Various solutions are available to meet customer and application needs.</p> <p>Mainframe storage is available through:</p> <ol style="list-style-type: none"> <li>1. Disk – fully redundant, fastest recovery.</li> <li>2. Tape – using automated tape library.</li> </ol> <p>Options: Customers may opt for:</p> <ol style="list-style-type: none"> <li>1. Dedicated storage: Storage on individual equipment or disk accessible by a single host.</li> <li>2. Custom usage reporting – Designed reports to meet the needs of the individual customer.</li> </ol>
d. Service prerequisites	Hosting service or state network access.
e. Description of what is not included in the service	Backup services are provided separately from the storage service.

## 2. How is the service requested?

a. Service request options:	<p>Services are requested through IVANTI, the DCS secure on-line support system, at <a href="https://oregondcsesm-amc.ivanticloud.com">https://oregondcsesm-amc.ivanticloud.com</a>. New customers may Contact an Account Manager @ 503-378-6758 or email <a href="mailto:DCS.Info@das.oregon.gov">DCS.Info@das.oregon.gov</a></p>
-----------------------------	--

b. What forms are used/needed to request this service?	Online general request form on IVANTI.
c. When can you expect to have your service request fulfilled?	Most storage services can be delivered within 30 days. Some environments may take more or less time depending on complexity.
<b>3. How do I get help? How does the program/Service Enterprise provide support to customers of this service?</b>	
a. Self-service support	There is currently no self-service support for this service.
b. Requesting support	<p>If experiencing a disruption of service or severe degradation of service, call 503- 373-1000 (DCS Service Desk) or Submit an Incident through IVANTI</p> <p>For changes or modifications to the service, use the general request process through IVANTI.</p>
c. When can you expect to get a response?	<p>DCS follows standardized response times for all services. Customers should expect DCS staff to respond within the following time frames:</p> <ul style="list-style-type: none"> <li>Severity 1 service disruptions – 15 minutes</li> <li>Severity 2 service disruptions – 60 minutes</li> <li>Severity 3 service disruptions – 1 business day</li> <li>Severity 4 service disruptions – 2 business days</li> <li>Requests for changes or modifications– 3 business days</li> </ul> <p>Severity levels for service disruptions are determined by the scope and impact of the individual incident. See incident response section of SLA for description of severity levels.</p>

# IT Professional Services

1. What is the service?	
a. Service Summary	IT professional services provide general technical support, and consulting to meet customer short-term technology needs.
b. Description of the features and benefits of the service	<p>The base service provides an hourly IT resource and may be engaged in two ways:</p> <ol style="list-style-type: none"> <li>1. A request for a resource to accomplish specific tasks or activities, such as consulting or project management.</li> <li>2. A request for a task or activity to be performed, such as a customer request to modify a firewall.</li> </ol>
c. Offerings and options	<p>Resources can be provided for:</p> <ol style="list-style-type: none"> <li>1. General technical expertise/support – Resource performs IT work for the customer. These requests may be submitted for a specific task to be completed or for a resource such as an application development.</li> <li>2. Technical consulting – Resource recommends how IT work should be performed. These requests would generally be submitted as a request for consulting relating to a specific IT-related situation such as recommendation in designing a network.</li> </ol>
d. Service prerequisites	None.
e. Description of what is not included in the service	Hardware, software, or any goods that are required to implement an IT solution is not provided as part of this service.
2. How is the service requested?	
a. Service request options:	<p>Services are requested through IVANTI, the DCS secure on-line support system, at <a href="https://oregondcsesm-amc.ivanticloud.com">https://oregondcsesm-amc.ivanticloud.com</a>. New customers may Contact an Account Manager @ 503-378-6758 or email <a href="mailto:DCS.Info@das.oregon.gov">DCS.Info@das.oregon.gov</a></p>
b. What forms are used/needed to request this service?	Online general request form on IVANTI.

<p>c. When can you expect to have your service request fulfilled?</p>	<p>Because of the variety of requests for IT professional services, fulfillment of the request will vary depending on the needs.</p> <p>Most simple requests can be delivered within 5 days if the requirements of the work are specified. More complex or longer-term requests, such as a request for project manager services, will take longer to initiate and will depend on the availability of a resource and the needs of the requester.</p>
<p><b>3. How do I get help? How does the program/Service Enterprise provide support to customers of this service?</b></p>	
<p>a. Self-service support</p>	<p>There is currently no self-service support for this service.</p>
<p>b. Requesting support</p>	<p>If experiencing a disruption of service or severe degradation of service, call 503- 373-1000 (DCS Service Desk) or Submit an Incident through IVANTI</p> <p>For changes or modifications to the service, use the general request process through IVANTI.</p>
<p>c. When can you expect to get a response?</p>	<p>DCS follows standardized response times for all services. Customers should expect DCS staff to respond within the following time frames:</p> <ul style="list-style-type: none"> <li>Severity 1 service disruptions – 15 minutes</li> <li>Severity 2 service disruptions – 60 minutes</li> <li>Severity 3 service disruptions – 1 business day</li> <li>Severity 4 service disruptions – 2 business days</li> <li>Requests for changes or modifications– 3 business days</li> </ul> <p>Severity levels for service disruptions are determined by the scope and impact of the individual incident. See incident response section of SLA for description of severity levels.</p>

# Colocation

## 1. What is the service?

<p>a. Service Summary</p>	<p>Colocation services provide a secure location in an access-controlled facility for housing servers and related equipment that customers own and manage. This service can be utilized for production systems or assist with disaster recovery, redundancy and backups, and provide a physical space for proprietary equipment to be located with hosted applications. 24/7 unescorted access is granted to colocation customers.</p>
<p>b. Description of the features and benefits of the service</p>	<p>Colocation facilities offer physical space for customer-owned equipment and include:</p> <ol style="list-style-type: none"> <li>1. Robust physical security and access control, including 24 hours video surveillance.</li> <li>2. 24/7 unescorted access utilizing a DAS-issued badge</li> <li>3. Fire detection and extinguishing devices.</li> <li>4. Multiple power feeds.</li> <li>5. Uninterruptable and filtered power, with backup power generators.</li> <li>6. Redundant air-conditioning.</li> <li>7. Staff and automated 24x7 monitoring of environmental and physical security.</li> <li>8. Cabinet access, power consumption and environmental reports.</li> <li>9. Flat rate billing all-inclusive of power consumption and access.</li> </ol>
<p>c. Offerings and options</p>	<p>Customers can choose from:</p> <ol style="list-style-type: none"> <li>1. Caged floor space for a higher level of security.</li> <li>2. Network connectivity model</li> <li>3. Staging room reservation and utilization</li> </ol>
<p>d. Service prerequisites</p>	<p>Network access to the colocation facility.</p>



<p>e. Description of what is not included in the service</p>	<ol style="list-style-type: none"> <li>1. Management, maintenance, or monitoring of the colocated equipment or applications on the equipment.</li> <li>2. Rack mounting kits, cable management and rack accessories are not included. Cage nuts and blanking panels are provided.</li> </ol>
<p><b>2. How is the service requested?</b></p>	
<p>a. Service request options:</p>	<p>Services are requested through IVANTI, the DCS secure on-line support system, at <a href="https://oregondcsesm-amc.ivanticloud.com">https://oregondcsesm-amc.ivanticloud.com</a>. New customers may Contact an Account Manager @ 503-378-6758 or email <a href="mailto:DCS.Info@das.oregon.gov">DCS.Info@das.oregon.gov</a></p>
<p>b. What forms are used/needed to request this service?</p>	<ol style="list-style-type: none"> <li>1. Colocation Cabinet request on IVANTI.</li> <li>2. Colocation Customer Badge Access request on Ivanti.</li> <li>3. Badge Access Request form provided by the Colocation Architect.</li> </ol>
<p>c. When can you expect to have your service request fulfilled?</p>	<p>Standard delivery of a colocation rack is 3 business days. Badge access is granted within 5 business days. Network connectivity is not included in the delivery of a rack and are requested separately.</p>
<p><b>3. How do I get help? How does the program/Service Enterprise provide support to customers of this service?</b></p>	
<p>a. Self-service support</p>	<p>There is currently no self-service support for this service.</p>
<p>b. Requesting support</p>	<p>If experiencing a disruption of service or severe degradation of service, call 503- 373-1000 (DCS Service Desk) or Submit an Incident through IVANTI</p> <p>For changes or modifications to the service, use the general request process through IVANTI.</p>
<p>c. When can you expect to get a response?</p>	<p>DCS follows standardized response times for all services. Customers should expect DCS staff to respond within the following time frames:</p> <ul style="list-style-type: none"> <li>Severity 1 service disruptions – 15 minutes</li> <li>Severity 2 service disruptions – 60 minutes</li> <li>Severity 3 service disruptions – 1 business day</li> <li>Severity 4 service disruptions – 2 business days</li> <li>Requests for changes or modifications– 3 business days</li> </ul> <p>Severity levels for service disruptions are determined by the scope and impact of the individual incident. See incident response section of SLA for description of severity levels.</p>

# Hosting

## 1. What is the service?

<p>a. Service Summary</p>	<p>DCS engineers, builds, and supports customized hosting solutions designed to help customers improve IT quality, efficiency, and reliability. Depending on infrastructure needs, DCS can virtualize existing servers, build an entire custom hosted infrastructure, or simply provide a managed server. DCS' wide array of professional capabilities to provide the right solution to meet customers' needs.</p>
<p>b. Description of the features and benefits of the service</p>	<p>Hosting services provide the technical infrastructure and support services for customers to install, operate and maintain their applications and services on a variety of operating system platforms.</p> <p>The base service includes:</p> <ol style="list-style-type: none"> <li>1. Infrastructure and operating system to host the customer application or system.</li> <li>2. Infrastructure and operating system management and administration.</li> <li>3. Network connectivity within the state's Data Center.</li> <li>4. Secure access control.</li> <li>5. Operating system monitoring.</li> </ol> <p>DCS can customize services to meet the individual requirements of the customer.</p>
<p>c. Offerings and options</p>	<p>Hosting services are available on the following operating system platforms:</p> <ol style="list-style-type: none"> <li>1. Mainframe             <ul style="list-style-type: none"> <li>• z/OS</li> </ul> </li> <li>2. Midrange:             <ul style="list-style-type: none"> <li>• Unix</li> <li>• iSeries</li> </ul> </li> <li>3. Server:             <ul style="list-style-type: none"> <li>• Linux</li> <li>• Windows</li> </ul> </li> <li>4. Middleware:             <ul style="list-style-type: none"> <li>• WebSphere</li> <li>• ColdFusion</li> <li>• Oracle Application Services</li> </ul> </li> </ol> <p>Options: Additional options that the customer may choose to include:</p>

	<ol style="list-style-type: none"> <li>1. Data storage.</li> <li>2. Backup, including off-site storage.</li> <li>3. Disaster recovery – Recovery or continuation of the technology infrastructure, not the customer application or system, in the event of a natural or human- induced disaster.</li> <li>4. Application monitoring – Performance monitoring of the customer application or system.</li> <li>5. Batch monitoring and job scheduling – Scheduling and monitoring of computing functions that run in the background of a customer application or system.</li> <li>6. Hosting at customer site – An operating system platform provided at a site requested by the customer rather than the State Data Center.</li> <li>7. Secure data transfer – Encryption and authentication to ensure that data is concealed in transit and that the sending and receiving systems are the intended systems.</li> <li>8. Test and development operating systems – Operating systems platforms for the application or system developers to use prior to the application or system being place in production for use.</li> </ol>
d. Service prerequisites	<ol style="list-style-type: none"> <li>1. All customer applications and systems be appropriately licensed.</li> <li>2. State network access (See state network access for description).</li> <li>3. Compliance with requirements of <a href="#">Statewide IT Policy 107-004-130</a>, Information Technology Investment Review/Approval if appropriate.</li> </ol>
e. Description of what is not included in the service	<ol style="list-style-type: none"> <li>1. Customer application or system to be installed.</li> <li>2. Customer application or system configuration.</li> <li>3. Development, debugging or maintenance of customer application or system.</li> <li>4. Administration of the customer application.</li> <li>5. Installation of the application or system.</li> <li>6. Migration of customer data.</li> <li>7. De-installation of customer applications, systems, or data.</li> </ol>
<b>2. How is the service requested?</b>	
a. Service request options:	<p>Services are requested through IVANTI, the DCS secure on-line support system, at <a href="https://oregondcsesm-amc.ivanticloud.com">https://oregondcsesm-amc.ivanticloud.com</a>. New customers may Contact an Account Manager @ 503-378-6758 or email <a href="mailto:DCS.Info@das.oregon.gov">DCS.Info@das.oregon.gov</a></p>

b. What forms are used/needed to request this service?	Online general request form on IVANTI.
c. When can you expect to have your service request fulfilled?	<p>Most hosting options can be delivered within the timeframes listed below:</p> <ol style="list-style-type: none"> <li>1. Mainframe           90 days</li> <li>2. Midrange           60 days</li> <li>3. Middleware         30 days</li> <li>4. Servers             30 days for virtual servers                               90 days for physical servers</li> </ol> <p>Some set ups may take more or less time depending on complexity.</p>
<b>3. How do I get help? How does the program/Service Enterprise provide support to customers of this service?</b>	
a. Self-service support	There is currently no self-service support for this service.
b. Requesting support	<p>If experiencing a disruption of service or severe degradation of service, call 503- 373-1000 (DCS Service Desk) or Submit an Incident through IVANTI</p> <p>For changes or modifications to the service, use the general request process through IVANTI.</p>
c. When can you expect to get a response?	<p>DCS follows standardized response times for all services. Customers should expect DCS staff to respond within the following time frames:</p> <ul style="list-style-type: none"> <li>Severity 1 service disruptions – 15 minutes</li> <li>Severity 2 service disruptions – 60 minutes</li> <li>Severity 3 service disruptions – 1 business day</li> <li>Severity 4 service disruptions – 2 business days</li> <li>Requests for changes or modifications– 3 business days</li> </ul> <p>Severity levels for service disruptions are determined by the scope and impact of the individual incident. See incident response section of SLA for description of severity levels.</p>

# Cloud Services

## 1. What is the service?

<p>a. Service Summary</p>	<p>The role of DCS as a service provider is to enable agency IT divisions, developers, and end-users to quickly access and deploy cloud environments with minimal friction and IT overhead while maintaining effective guardrails in terms of centralized policies and procedures that leverage pre-built templates. This represents a fundamental shift from the traditional approaches to providing centralized IT infrastructure.</p> <p>State agencies have varying levels of support needed from the DCS Cloud Services. DCS has established a tiered approach to accommodating the various levels.</p> <ul style="list-style-type: none"> <li>• Native Cloud Offering – Core Enterprise Organization Cloud Framework with security services and available private transit to State of Oregon network</li> <li>• EIS-Managed Cloud Offering – Native Cloud Offering plus DCS Compute services within the cloud environment</li> </ul>
<p>b. Description of the features and benefits of the service</p>	<ul style="list-style-type: none"> <li>• Cloud Services Brokering – Establishes a relationship with cloud providers</li> <li>• Identity and Access Management – utilizes Azure Active Directory services to provide single sign-on, MFA and other authentication services</li> <li>• DCS-Managed Compute Services – Linux and Windows virtual servers hosted in the cloud and managed by DCS compute teams</li> <li>• Customer-Managed Resources – consume and self-manage the Cloud Service Providers catalog offerings</li> <li>• Connectivity – private transit and State-managed Internet services connecting the State network to the Cloud Service Provider</li> <li>• Consultation – provided by DCS or initiate consultation engagements with the reseller or Cloud Service Provider</li> <li>• Vendor Relationship Management – a portfolio of DAS procured contracts and price agreements for cloud services with well-defined responsibilities of the Cloud Service Provider</li> <li>• Network Security – Cloud-hosted firewalls</li> <li>• Billing Structure – Direct billing to agency from Cloud Service Provider reseller</li> <li>• Customer Landing Zones – Agency separated cloud spaces in the enterprise framework within the Cloud Service Provider’s service.</li> </ul>

	<ul style="list-style-type: none"> <li>• Subscriptions, Projects, and Accounts – Billing containers to provide separation within the customer’s cloud spaces, including sandbox, development, test, staging and production.</li> <li>• Security Groups and Roles – Role-based Access Controls (RBAC) to managed secure access with least privilege.</li> <li>• Automation – Implement state-wide security standards and expedite routine work for improved efficiencies within the service.</li> <li>• Architecture Strategy – PaaS, IaaS, Hybrid models</li> <li>• Alerts and Monitoring – DCS monitoring of DCS-managed cloud-hosted servers or utilize cloud-native monitoring offered by the Cloud Service Provider.</li> </ul>
<p>c. Offerings and options</p>	<p>All offerings within the DCS Cloud Service include:</p> <ul style="list-style-type: none"> <li>• Enterprise Framework within the cloud including agency cloud spaces</li> <li>• Cloud Service Provider’s catalog of services</li> </ul> <p>Native Cloud Offering</p> <ul style="list-style-type: none"> <li>• PaaS, IaaS and hybrid models</li> </ul> <p>EIS-Managed Cloud Offering</p> <ul style="list-style-type: none"> <li>• DCS-managed or customer-managed server resources (RAM, CPU, etc.)</li> <li>• Linux or Windows operating systems</li> </ul>
<p>d. Service prerequisites</p>	<p>Before requesting DCS Cloud Services, the following must be completed:</p> <ul style="list-style-type: none"> <li>• Cloud provider contract in place</li> <li>• Privileged Access accounts</li> <li>• Customer on-boarding into DCS systems (billing, Ivanti)</li> <li>• Customer of DCS’ Azure Active Directory service</li> </ul>
<p>e. Description of what is not included in the service</p>	<p>The following items not included are available from the Cloud Service Provider’s catalog but not provided by EIS directly.</p> <p>Native Cloud Offering</p> <ul style="list-style-type: none"> <li>• DCS-managed virtual servers</li> </ul> <p>EIS-Managed Cloud Offering</p> <ul style="list-style-type: none"> <li>• Cloud native resources (i.e. serverless services, SQL instance)</li> </ul> <p>Excluded from DCS Cloud Services</p> <ul style="list-style-type: none"> <li>• Disaster Recovery and Service Continuity</li> <li>• Supporting infrastructure (such as VMware or technologies associated with managing core infrastructure).</li> </ul>

<b>2. How is the service requested?</b>	
a. Service request options:	Services are requested through IVANTI, the DCS secure on-line support system, at <a href="https://oregondcsesm-amc.ivanticloud.com">https://oregondcsesm-amc.ivanticloud.com</a> . New customers may Contact an Account Manager @ 503-378-6758 or email <a href="mailto:DCS.Info@das.oregon.gov">DCS.Info@das.oregon.gov</a> .
b. What forms are used/needed to request this service?	The forms required are dependent on the level of service requested. They may include: <ul style="list-style-type: none"> <li>• Privileged Access documentation</li> <li>• System Requirements Document</li> <li>• Cloud Calculator for specific Cloud Service Provider</li> <li>• EIS oversight documentation</li> </ul>
c. When can you expect to have your service request fulfilled?	Cloud Customer Onboarding: 5 business days DCS-Managed Cloud-Hosted VM: 3 business days Cloud Services Consultation: Variable 1 month to 1 year
<b>3. How do I get help? How does the program/Service Enterprise provide support to customers of this service?</b>	
a. Self-service support	Cloud Service Provider portal for resource and server management Reseller for consultation and technical support Knowledge articles available in Ivanti at the DCS Customer Portal Cloud Service Provider training courses DCS Cloud team support request
b. Requesting support	If experiencing a disruption of service or severe degradation of service, call 503- 373-1000 (DCS Service Desk) or Submit an Incident through IVANTI  For changes or modifications to the service, use the Cloud Other Services request through IVANTI. Contact information for the cloud services reseller and the Cloud Service Provider can be found in the DAS procurement contract visible on OregonBuys.gov.
c. When can you expect to get a response?	DCS follows standardized response times for all services. Customers should expect DCS staff to respond within the following time frames: <ul style="list-style-type: none"> <li>Severity 1 service disruptions – 15 minutes</li> <li>Severity 2 service disruptions – 60 minutes</li> <li>Severity 3 service disruptions – 1 business day</li> <li>Severity 4 service disruptions – 2 business days</li> <li>Requests for changes or modifications– 3 business days</li> </ul> <p>Severity levels for service disruptions are determined by the scope and impact of the individual incident. See incident response section of SLA for description of severity levels.</p>

# Appendix A

# DCS Managed Services Customer and DCS Roles & Responsibilities

Version 2

January 2023

## Revision History

Date	Version	Description	Author
03/01/2021	0.1	Initial Draft	AM Team
04/12/2021 – 06/29/2021	0.2 - 0.8	Various Edits incorporating manager and SME feedback	AM Team
07/01/2021	.9	Incorporated all manager feedback; PA feedback is pending	Eric Valdez
07/01/2021	1	Final Copy	Eric Valdez
01/01/2023	2	Updated to include Cloud services	AM Team



## 1. Executive Summary

Data Center Services (DCS) strives to serve the citizens of Oregon by providing technology services that enable and support the missions of our customers. To make those services available, there are many specific and/or shared roles and responsibilities that DCS and customers have. The purpose of this document is to articulate roles & responsibilities between DCS and customers for DCS service offerings, and is intended to be a guide to assist in high quality service delivery.

## 2. Operational Support

For urgent issues, agency is to call the DCS ServiceDesk at 503-373-1000. For lower-level severity issues, you can create in Incident Request in IVANTI.

IVANTI is the customer portal for submitting requests to the Data Center. It can be found at <https://oregondcsesm-amc.ivanticloud.com>.

## 3. Service Roles & Responsibilities

Below is a list of expectations for both the customer as well as Data Center technicians, when requesting services or support.

### 3.1 Linux

Task	Customer	DCS
<b>General</b>		
Approve all software beyond that provided in the standard build.	✓	
Review software configuration and installation standards for software or application configurations not provided in the standard build.	✓	
Configure and install operating system software and associated packages.		✓
Perform routine housekeeping and system maintenance activities.		✓
Start and stop processes that require privileged access as requested by the customer and as required by documented procedures.		✓
Customer staff or approved contractors may be able to start and stop specific services based on approval of a privileged access request.	✓	
Use Change Management process to schedule server maintenance.		✓
Use Change Management process to schedule application maintenance/upgrades.	✓	
Use Change Management process to provide notification of emergency changes.	✓	✓
Approve or deny in a timely fashion the installation of new OS releases, upgrades, and patches.	✓	
Approve or deny in a timely fashion the installation of emergency or urgent OS releases, upgrades and patches related to an exploitable security fix.		✓
Install new OS releases, upgrades, and patches.		✓
Support OS software.		✓
Support application software.	✓	
Migrate applications from unsupported operating system (to new OS) and manage application versions.	✓	
Maintain OS related documentation (e.g., build, standards, etc.).		✓
Maintain application software documentation.	✓	
Provide and implement monitoring processes and/or tools for operating system and DCS supported tools.		✓
Use automated system software tools and/or procedures to proactively monitor,		✓

manage and report on server performance.		
Perform proactive fault detection and diagnostic procedures.		✓
Determine server vs. application issues.	✓	✓
Monitor application availability.	✓	
Monitor/recommend tuning of performance of all servers.		✓
Provide outage notification of failed hardware and DCS managed software/middleware.		✓
Respond to audit requirements.	✓	✓
Set user and file permissions.		✓
Provide operating system-level account management.		✓
Track accounts and revoke unused accounts in a timely manner.	✓	
Track server license compliance that applies to operating systems and DCS system management tools.		✓
Track application software license compliance.	✓	
Troubleshoot and solve problems with hardware, OS, and supported software.		✓
Provide 24x7 on-call support for critical servers.		✓
Coordinate acquisition of vendor software, engaging DCS when appropriate.	✓	
Acquire SSL certificates as appropriate.		✓
Forecast resource requirements and share with DCS when major increases or decreases are planned.	✓	
Identify hardware/software (CPU, memory) needs.	✓	
Configure hardware/software installation/upgrades.		✓
Provide and implement application monitoring processes and tools.	✓	
Identify all authorized users.	✓	
Provide access to authorized users.		✓
Deploy roles from Proven Deployment Templates.		✓
Install application(s) on server.	✓	
Install and test application patches.	✓	
Monitor application performance.	✓	
Support remote access users.	✓	
Keep customer contact information current.	✓	
Keep systems administrator contact information current.		✓
<b>Data Management</b>		
Identify storage requirements.	✓	
Manage storage assets.		✓
Identify data that will be backed up.	✓	
Provide data retention requirements.	✓	
Approve backup and recovery strategy.	✓	
Install client software on servers to facilitate data backup.		✓
Restore/recover data at server level, if necessary.		✓
Assist customer restore individual files.		✓
Assist customer to do ad-hoc backups as requested.		✓

### 3.2 Windows

Task	Customer	DCS
<b>Build/Delivery</b>		
Identify business requirements.	✓	
Identify technical requirements.	✓	
Cost estimate.		✓
Budgetary approval.	✓	
Generate system requirement document.	✓	
Enter CUSTOMER PORTAL request.	✓	
Capacity review (determine physical or virtual, if virtual UCP or other virtual farm, if physical it's an exception).		✓
Generate system design.		✓
Send system design out for approval to agency.		✓
Approval of design.	✓	
Generate final approved system design.		✓
Provision (install O/S, server build).		✓
Enter request to set up patching, AV, monitoring.		✓
Install roles (SQL).		✓
Quality control - checklist (standalone or cluster).		✓
Delivery notification.		✓
Agency system validation.	✓	
Agency system hardening.	✓	
Delivery request closed.		✓
Add server to patching schedule* requires agency input (e.g., special patching instructions).		✓
Enter request to enable monitoring (e.g., What's Up Gold, Nagios, NetScout, etc.).		✓
Enter request/contact Account Manager to enable agency specific monitoring (e.g., zz-critical servers, circuits, sites, etc.).	✓	
Determine backup schedule (e.g., retention, custom schedule).	✓	
Enter request to set backup schedule.		✓
<b>Support</b>		
SQL patching.	✓	
Backup/restore (DB) - local.	✓	
Server level restore.		✓
Service disruption - initial troubleshooting/fix.	✓	
Service disruption – escalation.		✓
SQL cluster failover.	✓	
Add server resources (memory, CPU, storage, etc.).		✓
Additional OS/SQL component installation.	✓	✓
Server reboots.	✓	✓
<b>Server Health</b>		

Monitor and Manage disk space (allocation, decreases, and increases).	✓	✓
O/S patching.		✓
Manage VM/Server Health.		✓
Monitoring (O/S) - up/down.	✓	✓
VM patching/upgrade.		✓
Monitor backup failures.	✓	
<b>SQL Health</b>		
Monitor and Manage SQL Services Up/Down.		✓
SQL Database Management.	✓	
Server Performance (CPU, memory, disk I/O, SQL counters).	✓	
Maintenance jobs (integrity check, backups, index maintenance, statistics update).	✓	
<b>SQL Configuration</b>		
Instance settings.	✓	
Memory.	✓	
TempDB.	✓	
File locations.	✓	
File growth settings.	✓	
Service account password maintenance (password changes/tracking).	✓	
Creation of required jobs.	✓	
Feature enablement.	✓	
Security (mixed vs. windows only).	✓	
Monitor schema changes.	✓	
Monitor security changes, DB & object owners.	✓	
Collation DB level.	✓	
Collation instance level.		✓
DB creation/settings.	✓	
DB decommission.	✓	
Object creation/deletion.	✓	
User account creation.	✓	
Proxy account creation.	✓	
Proxy account configuration.	✓	
Credential creation.	✓	
SSIS catalog creation/configuration.	✓	
SSRS configuration.	✓	
Log shipping configuration.	✓	
SQL DB upgrade.	✓	
SQL DB migration.	✓	
Replication.	✓	
<b>Availability Groups</b>		
Request new Listener (separate from initial installation) creation.	✓	
Listener creation (new) in AD.		✓
IP request (new, separate from initial installation).	✓	

IP assigned.		✓
Availability group configuration.	✓	

### 3.3 Disaster Recovery/System Recovery

Responsible for providing the infrastructure.		✓
Responsible for restoring the Operating System (OS) and OS configurations to match pre-disaster environment.		✓
Responsible for restoring the application and all application/customer data onto the system.	✓	
Server restore to Master Design documentation.		✓
Rebuild server.		✓
Database restores.	✓	
File restores (o/s, system).		✓
File restores - business data.	✓	

### 3.4 Active Directory

Task	Customer	DCS
<b>Production</b>		
IP Subnet reservation and DNS configuration.	✓	
Domain management (domain controllers, sites & services, etc.).	✓	
OU structure.	✓	
Default group policy (security baseline).		✓
Group policy changes and additions (agency based).	✓	
Group policy change review (agency based).		✓
Domain membership of servers.		✓
Management of groups, users, and delegation.	✓	
DCS staff user object sync to Prod AD (Quick connect config and service).		✓
<b>DMZ</b>		
IP subnet reservation and DNS configuration.		✓
Domain management (domain controllers, sites & services, etc.)		✓
OU structure.		✓
Group policy.		✓
Domain membership of servers.		✓
Management of groups and users.	✓	
<b>Windows Server Patching</b>		
Provide summary of patches.		✓
Provide schedule for patches.		✓
Provide and/or install patches.		✓
Communication in relation to patches.		✓
Manage and maintain patch management infrastructure.		✓
Patch compliance.	✓	✓

Patch compliance reports.		✓
Firewall rule maintenance as it pertains to patching.		✓
Maintenance of patching documentation.		✓
Ensuring servers are rebooted after patching where needed.	✓	
Report patch scheduling conflicts and reschedule.	✓	
Application maintenance prior to patching.	✓	
OS hardening testing and implementation after completion of patching.	✓	
OS/application testing during patching maintenance.	✓	
Management of server patching for excluded servers.	✓	

### 3.5 File and System Backup

Task	Customer	DCS
Define backup requirements and schedules.	✓	
Ensure backup requirements and schedules are defined to ensure restoration capability. For example, data may need to be synchronized to a specific point in time for systems that share data.	✓	
Define retention periods for backups.	✓	
Perform backup restoration.	✓	
Data classification of backed up data.	✓	
Provide management, monitoring and maintenance of backup equipment.		✓
Establish and execute backups based on customer requirements.		✓
Validate backups complete as planned.		✓
Validate data in system backups.	✓	
Test the validity of backup data.	✓	

### 3.6 DNS

DCS is responsible for IP address management though customers are granted the ability to view and update IP address data as needed.

**Internal (agency managed) DNS services:** These are zones and servers hosted and managed by the customer.

**Semi-internal DNS services:** These zones are partially internal (based on the Single Perimeter Firewall to the internet) and are available to other State agencies. These zones are hosted on the Enterprise DNS system and DCS is responsible for records management. Changes to this environment is based upon customer request via a CUSTOMER PORTAL general request.

**External DNS services:** These zones are hosted on the Enterprise DNS system with records made available to the public. DCS is responsible for records management. Changes to this environment is based upon customer request via a CUSTOMER PORTAL general request ticket.

Task	Customer	DCS
<b>Internal DNS Services</b>		
Provide DNS server information.	✓	
Configure forwarders to Enterprise DNS system.	✓	
<b>Semi-internal DNS Services</b>		
Manage changes to the environment.	✓	✓
<b>External DNS Services</b>		

Manager changes to the environment.		✓
-------------------------------------	--	---

### 3.7 Mainframe

Task	Customer	DCS
<b>General</b>		
Keep customer contact information current.	✓	
Keep systems administrator contact information current.		✓
Approve all software beyond that provided in the standard build.	✓	✓
Review software configuration and installation standards for software or application configurations not provided in the standard build.		✓
Configure and install operating system software and associated packages.		✓
Perform routine housekeeping and system maintenance activities as required and approved.		✓
Use Change Management process to schedule server maintenance.		✓
Use Change Management process to schedule application maintenance/upgrades.		✓
Use Change Management process for Emergency changes notification.	✓	✓
Approve or deny in a timely fashion the installation of new OS and middleware releases, upgrades, and patches unless it is related to an exploitable security fix.	✓	
Install new OS and middleware releases, upgrades, and patches.		✓
Support OS software.		✓
Support application software.		✓
Support migration from unsupported operating system and application versions.		✓
Maintain OS related documentation (e.g., build, standards, etc.).		✓
Maintain application software documentation.		✓
Provide and implement monitoring processes and/or tools.		✓
Use automated system software tools and/or procedures to proactively monitor, manage and report on server performance.		✓
Perform proactive fault detection and diagnostic procedures.		✓
Determine server vs. application issues.		✓
Monitor application availability.	✓	✓
Monitor/recommend tuning of performance of all servers.		✓
Provide outage notification of failed hardware and software.		✓
Respond to audit requirements.	✓	✓
Set user and file permissions.	✓	
Provide operating system-level account management.		✓
Track accounts and revoke unused accounts in a timely manner.	✓	✓
Track server license compliance that applies to operating systems.		✓
Track application software license compliance.		✓
Troubleshoot and solve problems with OS and supported software.	✓	✓
Enter request/contact Account Manager to enable agency specific monitoring (e.g., zz-critical servers, circuits, sites, etc.).	✓	
Provide 24x7 on-call support for critical servers.		✓

Coordinate acquisition of vendor software.		✓
Acquire SSL certificates as appropriate.		✓
Forecast resource requirements.	✓	✓
Identify hardware/software (CPU, memory) needs.		✓
Configure hardware/software installation/upgrades.		✓
Provide and implement application monitoring processes and tools.		✓
Identify all authorized users.	✓	✓
Install application(s).		✓
Install and test application patches.		✓
Monitor application performance.	✓	✓
Support remote access users.	✓	
<b>Privileged Access</b>		
Start and stop processes that require privileged access as requested by the customer and as required by documented procedures.		✓
Customer staff or approved contractors may be able to start and stop specific services based on approval of a privileged access request.	✓	
<b>Data Management</b>		
Identify storage requirements.	✓	✓
Manage storage assets.		✓
Identify data that will be backed up.	✓	
Provide data retention requirements.	✓	
Approve backup and recovery strategy.	✓	
Install client software on servers to facilitate data backup.		✓
Restore/recover data at server level, if necessary.		✓
Assist customer restore individual files.		✓
Assist customer to do ad-hoc backups as requested.		✓
Perform problem analysis as requested.		✓
Participate in problem analysis if needed.	✓	
Implement problem analysis recommendations as requested/assigned for respective areas of service responsibility.	✓	✓

### 3.8 iSeries

Task	Customer	DCS
<b>General</b>		
Keep customer contact information current.	✓	
Keep systems administrator contact information current.		✓
Approve all software beyond that provided in the standard build.	✓	
Review software configuration and installation standards for software or application configurations not provided in the standard build.	✓	
Configure and install operating system software and associated packages.		✓
Perform routine housekeeping and system maintenance activities as required and approved.		✓
Start and stop processes that require privileged access as requested by the		✓



customer and as required by documented procedures.		
Customer staff or approved contractors may be able to start and stop specific services based on approval of a privileged access request.	✓	
Use Change Management process to schedule server maintenance.		✓
Use Change Management process to schedule application maintenance/upgrades.	✓	
Use Change Management process for Emergency changes notification.	✓	✓
Approve or deny in a timely fashion the installation of new OS releases, upgrades, and patches unless it is related to an exploitable security fix.	✓	
Install new OS releases, upgrades, and patches.		✓
Support OS software.		✓
Support application software.	✓	
Support migration from unsupported operating system and application versions.	✓	
Maintain OS related documentation (e.g., build, standards, etc.).		✓
Maintain application software documentation.	✓	
Provide and implement monitoring processes and/or tools.		✓
Use automated system software tools and/or procedures to proactively monitor, manage and report on server performance.		✓
Perform proactive fault detection and diagnostic procedures.		✓
Determine server vs. application issues.	✓	✓
Monitor application availability.	✓	
Monitor/recommend tuning of performance of all servers.		✓
Provide outage notification of failed hardware and software.		✓
Respond to audit requirements.	✓	✓
Set user and file permissions.	✓	
Provide operating system-level account management.	✓	
Track accounts and revoke unused accounts in a timely manner.	✓	
Track server license compliance that applies to operating systems.		✓
Track application software license compliance.	✓	
Troubleshoot and solve problems with hardware, OS, and supported software.		✓
Provide 24x7 on-call support for critical servers.		✓
Coordinate acquisition of vendor software, engaging DCS when appropriate.	✓	
Acquire SSL certificates as appropriate.		✓
Forecast resource requirements.	✓	
Identify hardware/software (CPU, memory) needs.	✓	
Configure hardware/software installation/upgrades.		✓
Provide and implement application monitoring processes and tools.	✓	
Identify all authorized users.	✓	
Install application(s) on server.	✓	
Install and test application patches.	✓	
Monitor application performance.	✓	
Support remote access users.	✓	

<b>Data Management</b>		
Identify storage requirements.	✓	
Manage storage assets.		✓
Identify data that will be backed up.	✓	
Provide data retention requirements.	✓	
Approve backup and recovery strategy.	✓	
Install client software on servers to facilitate data backup.		✓
Restore/recover data at server level, if necessary.		✓
Assist customer restore individual files.		✓
Assist customer to do ad-hoc backups as requested.		✓
<b>Incident Management</b>		
Provide and maintain a single point of contact for the reporting and tracking of hardware or system software problems.		✓
Resolve requests from customer.		✓
Adhere to problem management escalation procedures.	✓	✓
Maintain current status on open problems.		✓
Report on problems within established timeframes.		✓
Perform problem analysis as requested.		✓
Participate in problem analysis if needed.	✓	
Implement problem analysis recommendations as requested/assigned for respective areas of service responsibility.	✓	✓

### 3.9 UNIX

<b>Task</b>	<b>Customer</b>	<b>DCS</b>
<b>General</b>		
Keep customer contact information current.	✓	
Keep systems administrator contact information current.		✓
Request/approve all software beyond that provided in the standard build.	✓	✓
Review software configuration and installation standards for software or application configurations not provided in the standard build.	✓	
Configure and install operating system software and associated packages.		✓
Perform routine housekeeping and system maintenance activities as required and approved.		✓
Start and stop processes that require privileged access as requested by the customer and as required by documented procedures. Customer staff or approved contractors may be able to start and stop specific services based on approval of a privileged access request.	✓	✓
Use Change Management process to schedule server maintenance.		✓
Use Change Management process to schedule application maintenance/upgrades.	✓	
Use Change Management process to provide notification of emergency changes.	✓	✓
Approve or deny in a timely fashion the installation of new OS releases, upgrades, and patches unless it is related to an exploitable security fix.	✓	
Install new OS releases, upgrades, and patches.		✓

Support OS software.		✓
Support application software.	✓	
Support migration from unsupported operating system and application versions.	✓	
Maintain OS related documentation (e.g., build, standards, etc.).		✓
Maintain application software documentation.	✓	
Provide and implement monitoring processes and/or tools.		✓
Use automated system software tools and/or procedures to proactively monitor, manage and report on server performance.		✓
Perform proactive fault detection and diagnostic procedures.		✓
Determine server vs. application issues.	✓	✓
Monitor application availability.	✓	
Monitor/recommend tuning of performance of all servers.		✓
Provide outage notification of failed hardware and software.		✓
Respond to audit requirements.	✓	✓
Set user and file permissions.		✓
Provide operating system-level account management.		✓
Track accounts and revoke unused accounts in a timely manner.	✓	
Track server license compliance that applies to operating systems.		✓
Track application software license compliance.	✓	
Troubleshoot and solve problems with hardware, OS, and supported software.		✓
Provide 24x7 on-call support for critical servers.		✓
Coordinate acquisition of vendor software, engaging DCS when appropriate.	✓	
Acquire SSL certificates as appropriate.		✓
Forecast resource requirements.	✓	
Identify hardware/software (CPU, memory) needs.	✓	
Configure hardware/software installation/upgrades.		✓
Provide and implement application monitoring processes and tools.	✓	
Identify all authorized users.	✓	
Provide access to all authorized users.	✓	✓
Deploy roles from Proven Deployment Templates.		✓
Install application(s) on server.	✓	
Install and test application patches.	✓	
Monitor application performance.	✓	
Support remote access users.	✓	
<b>Data Management</b>		
Identify storage requirements.	✓	
Manage storage assets.		✓
Identify data that will be backed up.	✓	
Provide data retention requirements.	✓	
Approve backup and recovery strategy.	✓	
Install client software on servers to facilitate data backup.		✓

Restore/recover data at server level, if necessary.		✓
Assist customer restore individual files.		✓
Assist customer to do ad-hoc backups as requested.		✓
<b>Incident Management</b>		
Provide and maintain a single point of contact for the reporting and tracking of hardware or system software problems.		✓
Resolve service disruptions/incidents from customer.		✓
Adhere to problem management escalation procedures.	✓	✓
Maintain status on open problems.		✓
Report on problems within established timeframes.		✓
Perform problem analysis as requested.		✓
Participate in problem analysis if needed.	✓	
Implement problem analysis recommendations as requested/assigned for respective areas of service responsibility.	✓	✓
Provide problem trend analysis.		✓

### 3.10 Network

Task	Customer	DCS
<b>Local Area Network (LAN)</b>		
Performance monitoring, management, and reporting of networking equipment, such as switches.		✓
Management of the logical network components – the communications protocols that create the system of digital message formats and rules for exchanging data, and including signaling, authentication and error detection and correction capabilities.		✓
Provision of IP addresses for use by customer devices. Except where customer is IPAM provider.		✓
Hardware and software lifecycle management for network equipment and components.		✓
Maintaining and managing of <i>Private</i> addresses for the LAN via DHCP.		✓
Management of customer devices, such as workstations and printers.	✓	
Management of customer device connections to the local area network.	✓	
Cabling infrastructure – jacks, copper and fiber cabling, patch panels.	✓	
Secure physical space for equipment, including power, and that is accessible to DCS staff.	✓	
UPS system for Agency’s critical sites – telco equipment, DCS router, DCS switches, VoIP phones, and PCs.	✓	
<b>State Network Access (WAN)</b>		
Performance monitoring, management, and reporting of networking equipment, such as switches.		✓
Hardware and software lifecycle management for network equipment and components.		✓
Assign unique private IP block for customer usage.		✓
Management of customer devices, such as workstations and printers.	✓	
Management of customer device connections to the local area network.	✓	

Off-net circuit connectivity for Agency specific communication needs.	✓	
Secure physical space for equipment, including power and accessible to DCS Staff.	✓	
Provide QOS services for VoIP devices.		✓
Network traffic monitoring through tools provided by DCS at the request of the customer.	✓	

### 3.11 Colocation

Task	Customer	DCS
Facilities Infrastructure Management (PDUs, racks, handles, etc.).		✓
Badge Management; Shared with DAS Facilities.		✓
Power System Management; Shared with DAS Facilities.		✓
Surveillance System Management.		✓
Physical Security with 24/7 Unescorted Access.		✓
Environmental Quality Management (temperature, humidity); Shared with DAS Facilities.		✓
DCIM Appliance and Application including reporting and event management.		✓
Provide a Staging Room.		✓
Customer Instance WAN Connectivity (Design, Implementation).	✓	✓
Customer Instance LAN Connectivity.	✓	✓
IT Systems Hardware (Purchase, Maintenance, Retirement, Incident and Change Management of servers, storage, security, and networking equipment).	✓	
Customer Rack to Rack Cabling.	✓	
Shipping/Receiving at the Data Center.	✓	✓
Badge Access Granting and Revocation.	✓	
System Design and Maintenance.	✓	
Regulatory Program Compliance.	✓	✓

### 3.12 Privileged Access

Task	Customer	DCS
<b>General Privileged Access</b>		
Complete CIO Privileged Access (PA) Agreement and submit.	✓	
Complete Privileged Access Agreement individual and store in personal file.	✓	
Create Windows PA User ID	✓	
Request Privileged Access for individual using Privileged Access Request form (CIO or Delegate).	✓	
Ensure that firewall request have been put in place for access of servers.	✓	
Review PA Submissions and ensure CIO or Delegate has submitted.		✓
Review PA Submissions for completeness.		✓
Submit Privileged Access Request.		✓
Create Linux PA User ID.		✓
Grant PA to individual user.		✓
Notify Agency of DCS users with PA capabilities.		✓

Notify DCS of agency users who should no longer have PA rights.	✓	
Audit of those with PA access, according to system records, compared to PA Access requests submitted.		✓
Revoke/removal of unused/expired Customer PA accounts.	✓	
Removal of unused/expired DCS PA accounts.		✓
<b>Linux Privileged Access</b>		
List Linux system where PA user will need access too.	✓	
Ensure that firewall request have been put in place for access to Linux servers.	✓	
<b>Windows Privileged Access</b>		
Ensure that the user's PA account is not disabled in Agency Active Directory.	✓	
Create PA Account in Agency Active Directory and make sure the user PA account fits with Agency's naming standard for PA accounts.	✓	
<b>Mainframe Privileged Access</b>		
Mainframe PA access done through agency Resource Access Control Facility (RACF) admin.	✓	

### 3.13 General Support

Task	Customer	DCS
<b>Incident Management</b>		
Provide agency distribution list name to DCS for all SEV-1 notices to be sent to.	✓	
Communicate SEV-1 notices to internal agency business units and/or customers that are impacted by the outage.	✓	
Provide & maintain a list of critical sites or resources for monitoring purposes.	✓	
Perform basic troubleshooting to ensure issues are not user error, application error, or issue caused by lack of utility power.	✓	
Provide and maintain a single point of contact for the reporting and tracking of hardware or system software problems.		✓
Resolve requests from customer.		✓
Adhere to problem management escalation procedures.	✓	✓
Maintain current status on open problems.		✓
Report on problems within established timeframes.		✓
Participate in problem analysis if needed.	✓	✓
Implement problem analysis recommendations as requested/assigned for respective areas of service responsibility.	✓	✓
Provide problem trend analysis.		✓
Perform problem analysis for all severity 1 incidents.		✓
Given a server name, determine what application(s) the agency uses that rely on that server.	✓	
<b>Change Management</b>		
Provide a distribution list name to DCS that to send all Change Management related items to. Includes, but is not limited to: Change Advisory Board (CAB) agenda and call-in number; Modifications to planned changes (RFCs).	✓	
Review Change Management emails and discuss planned changes, and modifications to planned changes, with internal business units that will/could be impacted by the planned change	✓	

Given a server name, determine what application(s) the agency uses that rely on that server.	✓	
--	---	--

### 3.14 DCS Cloud Services

Task	Customer	DCS
<b>Network Connectivity</b>		
Network Infrastructure and Connectivity		✓
<b>Cloud Servers</b>		
Server Build and Management	✓	✓
Serverless Compute	✓	
Compute Resilience and Optimization	✓	
Database Services	✓	
<b>Applications</b>		
Application Development	✓	
Application Performance Monitoring	✓	
<b>Data Management</b>		
Backup and Recovery	✓	
Storage	✓	
<b>Business Support</b>		
Regulatory Program Compliance		✓
Financial Analysis	✓	