Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Larry Hogan | Governor
Boyd K. Rutherford | Lt. Governor
Michael G. Leahy | Secretary
Lance Schine | Deputy Secretary

SERVICE AGREEMENT

Between
The Maryland Department of Information Technology and
User Agency
For
Server and Storage Services (FY2021)

This Service Agreement forms a part of the Memorandum of Understanding between the Maryland Department of Information Technology ("DoIT") and user agency ("Customer"). The parties agree as follows:

1 Services Covered

Server and Storage services is a model of cloud computing where IT services are provisioned over private IT hardware infrastructure hosted in the DoIT Data Center for a customer organization. The service is managed with internal DoIT staff IT resources. The infrastructure can be leveraged by a customer to host applications and services upon request. Additionally, customers receive the benefit of the Server Management Service (SMS) bundle to leverage the technical expertise of DoIT’s technical engineering team. The enterprise shared services bundle includes patch management, endpoint protection, network monitoring and a standardized network architecture. Server and Storage services includes but not limited to:

- Virtual Servers
- Operating System licenses (Windows or Linux)
- SQL database licenses
- Secure Socket Layer (SSL) Certificates
  - Act in the capacity of an intermediary certificate authority (CA) and will issue / revoke / re-issue SSL certificates as requested by the owner.
  - Track SSL certificate expiration dates and send automated reminders when applicable.
  - Provide the Agency with the information needed to request and renew SSL certificates.
- Network file storage (CIF)
- Load balancing
- Non-Standard Services for Legacy Systems
- Remote Desktop Server Client Access (Terminal Server)
- Remote Access Virtual Private Network (VPN)
  - VPN connectivity to desktops and/or servers.
  - Logins to VPN platform using multi-factor authentication (MFA).
  - Upgrades to agency VPN appliances.
  - Upgrades to layer 3 mobile devices (client) software for VPN.
  - SSL certificates (encryption) for all production appliances used for the VPN platform and related authentication platforms/infrastructure.

  - Two-factor/multi-factor authentication (MFA) as the default implementation, where applicable.
  - Note: In instances where MFA is unable to be implemented, exceptions can be discussed with written approval from an agency.
- DoIT will provide notice to the User Agency at least 5 days in advance of and planned maintenance.
- Server Management Services (end-point protection, server monitoring, patch management)
  - Ensure Systems are run on an operating system that is capable of supporting end-point protection software version supported by the provider.
  - Ensure Systems are run on an operating system that is capable of receiving and installing Microsoft Windows updates.
  - Ensure there is adequate free space on hosted servers.
  - Upon request, agencies can notify the Enterprise Shared Services Team that they would like server monitoring alerts and notifications sent to application owners or other staff as required.
- Secure data center facility that is SSAE18 Type 2 SOC II, PCI-DSS, GLBA and HIPAA compliant
  - N+1 redundant electrical design and distribution
  - 24x7x365 on-site personnel
  - Access restricted to authorized client personnel and Data Center employees
  - Axis IP-based interior and exterior surveillance cameras
  - Data Center cage access is controlled by HIP contactless access cards.
  - Mantraps for increased physical security
  - Automatic switching from primary to backup power supply
  - Single and three-phase power
  - Completely isolated ground system
  - Diesel generators with 48 hours of on-site fuel, supplemented with refueling contracts
  - Multiple power feed stations.

2 Parties Responsibilities

2.1 DoIT's Responsibilities:

DoIT shall provide:

- Perform server level administrative function from the operating system down into the virtual server hyper-visor and hardware infrastructure.
- Provide the facilities, personnel, equipment, software and other resources necessary to provide services.
- Storage Encryption provides full-disk encryption to all hosted virtual servers
- FISMA, HIPAA, PCI, Basel II, SB 1386, and E.U. Data Protection Directive 95/46/EC regulations using FIPS 140-2 validated hardware complaint drive encryption.
- Assurance that content will be treated as confidential by not disclosing content other than to DoIT employees and contractors for use only to the extent needed to deliver the services.

- Assurance that content will be returned or destroyed upon the expiration or cancellation of services or earlier upon the client's request.
- Process, store and use account information wherever hosting services are provided to enable product features, administer user and personalize experience, and otherwise support or improve the use of the hosting environment.
- Ensure that all employees have undergone fingerprint CJIS background checks.

2.2 DoIT Responsibilities for Non-Enterprise:

DoIT shall provide:

- Provide the facilities, personnel, equipment, software and other resources necessary to provide Private Cloud Hosting Services.
- Storage Encryption provides full-disk encryption to all hosted virtual servers
- FISMA, HIPAA, PCI, Basel II, SB 1386, and E.U. Data Protection Directive 95/46/EC regulations using FIPS 140-2 validated hardware complaint drive encryption.
- Assurance that content will be treated as confidential by not disclosing content other than to DoIT employees and contractors for use only to the extent needed to deliver the Cloud Services.
- Assurance that content will return or destroyed upon the expiration or cancellation of the Cloud Services or earlier upon the client's request.
- Process, store and use account information wherever hosting services are provided to enable product features, administer user and personalize experience, and otherwise support or improve the use of the Cloud Services hosting environment.
- Ensure that all employees have undergone fingerprint CJIS background checks

2.3 DoIT shall not be responsible for the following under this Service Agreement:

- Customer application support includes but is not limited to web sites and applications, databases, database administration, native database backup maintenance plans, COTs software applications, application upgrades or customizations and database encryption. Any associated technologies, software applications, specialized software, custom configurations (ex: host files updates or user profile management on Servers) used in conjunction with an application, delivery or presentation of the application.
- DoIT does not provide virtual server hypervisor console access.
- Agency’s remote devices and services (i.e. any devices not hosted within MD DoIT’s private cloud environment/data center). Examples include; physical or virtual servers, hypervisors, scanning devices, storage devices, server backup system, video camera systems, video streaming applications, and remotely provided network services (ex. print services, directory services, file services).
- DoIT will not procure, maintain or renew Oracle licenses.
- Agency secure file transfer systems.
- VoIP solutions that are not the Enterprise standard.
- Non-enterprise agency server level administrative function on the operating system.
- Provision or order network circuits needed to connect to the DoIT data center.

- Application and database migrations to new servers.
- SSL Certificates:
  - DoIT will not generate a certificate signing request (CSR) or have access to / manage the Agency's certificates' private keys.
  - DoIT will not install certificates on Agency's servers or appliances.
- Administrative support, management or operations of non-enterprise standard VPN solutions which includes but is not limited to administration, configuration, patching, updating, user account management, software and hardware contracts and associated licenses

2.4 User Agency's Responsibilities:

User Agency shall:

- Provide hardware and software specific to their hosted application to access and/or use cloud hosted applications. This will include any client specific URL address and associated certificates.
- Respond if requested to provide additional funding if application requirements are outside of the scope of a standard server build for example: an application requires all of the memory and processor available in a single virtual server host or an application requires a significant amount of storage in the multi-terabyte or petabyte range or an Oracle program requires licenses to meet specific license requirements.
- Ensure all non-standard server provisioning requests can be built on enterprise standard equipment.
- Assume responsibility for security directly related to the application. For example the encryption to personally identifiable information in a database. TDE encryption as detailed in the article by Microsoft will need to be followed in every instance where PII or HIPAA data is being stored.
- Assume responsibility for use of services by any user who accesses the hosting services environment with the Client's account credentials.
- Ensure services are not used in any jurisdiction for unlawful, obscene, offensive or fraudulent content or activity, such as advocating or causing harm, interfering with or violating the integrity or security of a network or system, evading filters, sending unsolicited , abusive or deceptive messages, viruses or harmful code, or violating third party rights.
- Be responsible for obtaining all necessary permissions to use, provide, store and process content in the hosted environment and grant DoIT permission to do the same.
- Ensure any client content and applications that are subject to governmental regulations or may require security measures beyond those supplied by DoIT will not input or provide such content or hosted application unless DoIT has first agreed in writing to implement additional required security measures.
- Procurement of the licenses needed to host Oracle programs in the data center. In addition licenses must meet Oracle programs licenses rules, regulation and guidance that need to run the development, test and/or production environments. (Note: guidance on Oracle program hosting is available in the Third Party Compute service)

- Install all database programs to suit their specifications. Native database backups are the responsibility of the customer.
- Non-enterprise agencies need to perform their own operating system administration.
- Application and database migrations to new servers. Migration of applications to new servers and/or the functionality of applications after a server upgrade. Customer would need to identify application testers in either event to confirm application functionality
- VPN
  - Provide DoIT Service Management Services Team with an up-to-date point of contact for approving employee access requests and account removals.
  - All user account management is performed by the agency.
  - Notify DoIT if additional VPN users will be added to the service beyond what was originally agreed to in SOW.
  - Purchase state laptops for employees requiring use of the VPN client access.
  - Utilize Microsoft and Apple operating systems currently supported by DoIT on state owned devices.
  - Utilize an acceptable version of endpoint antivirus protection that is current and has recent definition files.
  - If required, procure two (2) virtual routers to standardize network connectivity architecture. (Doit can provide costs for appliance upgrades as needed.)
  - For HTML5 configurations: Provide a list of resources that agency staff & State contractors will need access to through the VPN.
  - Full engagement from non-enterprise agency to carry out all activities within their respective networks to enable VPN to work.
  - Purchase a new VPN appliance if the maximum simultaneous user will be exceeded. (DoIT can provide costs for appliance upgrades as needed.)
- SSL Certificates:
  - A certificate signing request (CSR) for generating an SSL certificate request.
  - Ensure the domain name for the certificate (common name) is properly registered. DoIT may refuse to issue/approve certificates for nonexistent or unregistered domain names.
  - The CSR needs to be created on the same server or device that you plan to install the certificate on. The CSR contains information (e.g. common name, organization, country) that the Certificate Authority will use to create your certificate. Following the successful execution of this agreement, the Agency may contact the DoIT Service Desk to request a certificate. A link to the certificates self-service portal will be provided at that time, along with the CSR information that is required by our system.
  - The necessary information to the Enterprise Cloud Services team to confirm which type of SSL certificate the agency will need. (DoIT recommendation on SSL certs is to agencies to use SSL Premium certificates. Premium certificates provide an extra layer of security with monthly vulnerability scans against a site.)

  - Following receipt of the signed certificate from DoIT's CA, Agency shall install the certificate onto the server or device containing the private key.

3 Service Level Agreements

- Support Hours: 8AM - 5PM Monday - Friday
- Uptime: 99.9%
- Response time and resolution targets:
  - Priority 1 (P1) response time 2 hours, resolve time 4 hours
  - Priority 2 (P2) response time 4 hours, resolve time 2 days
  - Priority 3 (P3) response time 1 day, resolve time 3 days
  - Priority 4 & 5 (P4/P5) response time 2 days, resolve time 5 days
- Note: At times, it may be necessary to contact a vendor for assistance, thereby lengthening response times.

4 Maintenance Schedules

Windows updates and patches applied to servers the third week of every month Tuesday - Thursday from 7:00PM - 12:00AM. DoIT will provide notice to the User Agency at least 5 days in advance of any planned maintenance. DoIT will document a list of all weekly and monthly changes planned in order to limit disruption to the user agency's environment. DoIT may modify a service, without degrading its functionality or security features. Any change that affects the commercial terms of the services will not be effective until the next agreed renewal or extension. Changes to the hosting environment are not retroactive, they apply as of the effective date only to new orders or ongoing services that do not expire and renewals.

- Non-Enterprise Customers:
  - Server patching, end-point protection (anti-virus), server monitoring are not available.
- VPN Remote Access Maintenance Schedules
  - DoIT will provide advanced notifications through the Service Desk of any planned maintenance.

5 Support and Service Outages

Normal hours of operation for DoIT technical support staff are 8AM – 5PM Monday - Friday (excluding holidays).

6 Costs for Services

The cost of the covered services is outlined in DoIT's Cost Allocation Schedule, which is the DoIT Shared Services- Annual Invoice, for the current fiscal year.

7 Termination of Services

Agency must provide 60 days' advance written notice to terminate services.

* Represents Services provided to Enterprise customers only.