



GovDataHosting Cloud Platform

Service Catalog

Version 3.7 | Effective 01/01/2026



COMPLIANCE
DOCUMENTATION
MANAGEMENT SERVICE

Table of Contents

01	Managed Network and Infrastructure Services	3
	▶ Managed Network Service	4
	▶ Managed Firewall Service	4
	▶ Managed VPN Service	4
	▶ Managed Reverse Proxy / Load Balancing / WAF Service	4
	▶ Managed DNSSEC Service	5
	▶ Managed Backup Service	5
02	Managed Application Support Services	6
	▶ Basic Operating System Administration Service	7
	▶ Database Administration Service	7
	▶ Patch Management Service	7
	▶ Server/Application Monitoring	7
	▶ SSL Certificate Management Service	8
	▶ Drupal Core Administration Service	8
	▶ Microsoft Exchange Administration Service	8
	▶ Microsoft SharePoint Administration Service	8
	▶ Application Migration Service	9
03	Managed Security Compliance And Cyber Defense Services	10
	▶ Anti-Virus/Anti-Malware Management Service	11
	▶ Compliance Documentation Management Service	11
	▶ Managed Disaster Recovery Service	11
	▶ Managed Intrusion Detection Service	11
	▶ Managed Log Aggregation Service	11
	▶ Managed Vulnerability Scanning Service	12
	▶ Managed Incident Response and Tracking Service	12
	▶ Managed Continuous Monitoring Service	12
	▶ Configuration Management Service	12
	▶ Asset Management Service	12
	▶ System Security Assessment Service	12
	▶ Digital Forensics Service	13
	▶ Assigned Information System Security Officer (ISSO)	13
04	Value-Added Services	14

▶ ServiceDesk Portal Service	15
▶ Software License Provisioning Service	15
▶ Project Management Coordination Service	15
▶ System Design Service	15
▶ Cloud Readiness Assessment Service	15

05

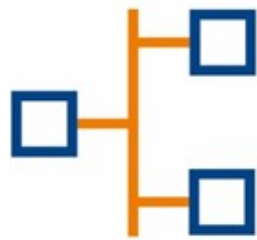
About Us 16

▶ About GovDataHosting	17
▶ Solutions	17
▶ Platforms	18
▶ Services	18
▶ Compliance & Contract Vehicles	18

01

GOVDATAHOSTING CLOUD PLATFORM MANAGED SERVICES

Managed Network and Infrastructure Services



MANAGED NETWORK
SERVICE





Managed Network Service

Management of basic customer networking components to include Virtual Private Cloud (VPC) and virtual/physical network interface setup, assignment and configuration of private/public IP addresses and customer Internet connectivity or private connection setup.



Managed Firewall Service

The GovDataHosting Firewall Service acts as the first layer of defense against unauthorized connections. To minimize vendor-dependent vulnerabilities, our enterprise Firewall Service is delivered utilizing native cloud firewalls. Management of inherited or dedicated network firewalls includes setup of deny all/allow by exception firewall traffic filtering rules based on port, protocol and service. All customer firewall configuration changes are required to be authorized by customer prior to implementation.



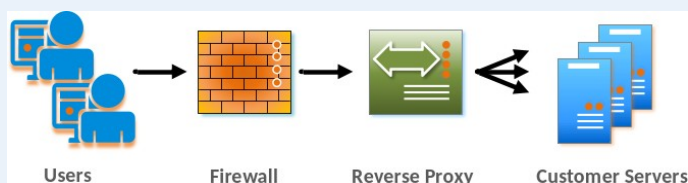
Managed VPN Service

Encrypted virtual private network (VPN) remote access connectivity with 2-factor authentication for privileged and basic users requiring administrative access to virtual servers utilizing our VPN access devices and the latest government FIPS approved encryption protocol with proper encryption key length. Customers do not have to have a dedicated VPN device to provision this service and can leverage our VPN remote access infrastructure as a cost-effective alternative to a dedicated solution. Service is limited to utilization of our VPN infrastructure. Customer-dedicated remote access VPN support requires a custom scope of work and on-going support. Additional shipping charges will apply for RSA/YubiKey token shipments to more than 3 customer geographic user locations per information system.



Managed Reverse Proxy / Load Balancing / WAF Service

Managed Reverse Proxy Service provides basic self-defending reverse proxy, traffic load-balancing and web application firewall (WAF) service utilizing the GovDataHosting Cloud Platform. This IP rule-based service serves as a cost-effective alternative to dedicated reverse proxy/load balancing/WAF solutions. Service is limited to utilization of our cloud infrastructure. Customer-dedicated reverse proxy/load balancer/WAF support requires a custom scope of work and on-going support.



MANAGED DNSSEC
SERVICE

Managed DNSSEC Service

Managed Domain Name System Security Extensions (DNSSEC) service provides customer-system oriented domain name resolution services through our managed DNS infrastructure. The purpose of this service is to provide protection against common vulnerabilities in the DNS protocol.

MANAGED BACKUP
SERVICE

Managed Backup Service

This service provides customers with a peace of mind that their data is periodically backed up and available for a restore if needed utilizing native cloud backup infrastructure. Depending on operating system utilized by the customer, our backup infrastructure is capable of restoring single files instead of having to restore an entire server to recover a single file. Managed backup and restoration services are available with a variety of incremental and full back up retention options to comply with OMB M-21-31 requirements.

02

GOVDATAHOSTING CLOUD PLATFORM MANAGED SERVICES

Managed Application Support Services



OPERATING SYSTEM
ADMINISTRATION SERVICE



OPERATING SYSTEM
ADMINISTRATION SERVICE

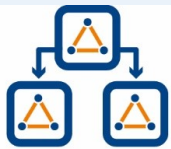
Basic Operating System Administration Service

Service supports Microsoft Windows Server, Ubuntu and Red Hat Enterprise Linux operating systems based on customer provisioned CPU, memory and disk resources. Service is limited to managing up to 10 privileged user or service accounts. Charges may apply for management of additional user/service accounts.

DATABASE ADMINISTRATION
SERVICE

Database Administration Service

Database installation, configuration, security compliance benchmark hardening and quarterly patching service. Support is available for Microsoft SQL Server, Oracle, Postgres, MariaDB and MySQL database management systems. DISA STIG and CIS database hardening benchmarks are available. Database administration tasking outside of the standard definition of Basic and Advanced Database Administration service type is not included in the scope of support, but may be available as a customer-specific support scope.

PATCH MANAGEMENT
SERVICE

Patch Management Service

Install vendor-provided patches for most of vendor supported and government authorized applications and open source products such as Microsoft, Ubuntu, Red Hat Enterprise Linux, Oracle, Apache and many more. Basic service offering includes installation of Microsoft or RHEL operating system patches, while the advanced offering includes patch installation for over 250+ applications.

Patches are installed during a customer-approved maintenance window. IT-CNP personnel provide an email notification in the beginning and end of the maintenance window so customers are aware when their system is being patched.

Mission critical customer systems designed with redundant functional components for high availability and load balancing purposes generally do not experience a service interruption for their customers as IT-CNPs systems patch each component of the information system separately from its high availability pier thus preserving service.

SERVER/APPLICATION
MONITORING SERVICE

Server/Application Monitoring

Basic and advanced set of computing resource, storage, database, and application performance monitoring services to accommodate the most demanding enterprise application performance requirements.


 SSL CERTIFICATE
MANAGEMENT SERVICE

SSL Certificate Management Service

Initial installation and on-going management of SSL certificate and related intermediary files. This service includes the provisioning of an SSL certificate through our certificate authority, logistics associated with getting the SSL certificate request issued and installed on customer and IT-CNP infrastructure tools, including customer's web servers, application servers and cloud services.

Government customers that have their own certificate authority (e.g. U.S. Department of Defense) can provide their own SSL certificates and intermediary files for management by IT-CNP.



Drupal

 DRUPAL ADMINISTRATION
SERVICE

Drupal Core Administration Service

Drupal core application installation and on-going Drupal core administration service including monthly health checks and quarterly security patches. This service includes applying zero-day critical security patches as soon as possible following customer approval.

Drupal content related services such as Drupal content publication, content management, theme design, module development, graphics/multi-media design, web visitor trend analysis and custom programming are not covered by this service, but are available from IT-CNP as a bundle through our partner network.


 EXCHANGE ADMINISTRATION
SERVICE

Microsoft Exchange Administration Service

Microsoft Exchange farm application installation and on-going farm administration service including Exchange administration feature settings, monthly health/performance log checks, issue troubleshooting and applying security patches on quarterly basis. This service includes applying zero-day critical security patches as soon as possible following customer approval.

Microsoft Exchange daily management tasking such as user account management, password resets, user helpdesk, user-specific configuration and related services are not covered by this service, but are available from IT-CNP as a bundle through our partner network.


 SHAREPOINT ADMINISTRATION
SERVICE

Microsoft SharePoint Administration Service

Basic Microsoft SharePoint farm application installation and on-going farm administration service including monthly health checks and quarterly application and security patches.



APPLICATION
MIGRATION SERVICE

Application Migration Service

IT-CNP utilizes lessons learned from hundreds of prior successful application migrations to ensure that customers leverage the latest best practices while managing risk associated with migrating their applications to the cloud.

03

GOVDATAHOSTING CLOUD PLATFORM MANAGED SERVICES

Managed Security Compliance And Cyber Defense Services



ANTI-VIRUS/MALWARE
MANAGEMENT SERVICE



ANTI-VIRUS/MALWARE
MANAGEMENT SERVICE

Anti-Virus/Anti-Malware Management Service

This service includes a centrally managed enterprise cloud anti-virus/anti-malware protection, including policy-driven Host Based Intrusion Detection System (HBIDS) per NIST SP 800-83 and application whitelisting.

COMPLIANCE DOCUMENTATION
MANAGEMENT SERVICE

Compliance Documentation Management Service

Basic and advanced security compliance documentation service to establish the minimally required initial system documentation by successfully completing system Assessment and Authorization (A&A) process, as well as maintaining on-going authorization through documenting the required periodic recurring tasks (documenting continuous monitoring activities).

DISASTER RECOVERY
SERVICE

Managed Disaster Recovery Service

Our Disaster Recovery Service offers customers a cost-effective disaster recovery strategy utilizing virtual server replication technologies and transmitting encrypted copies of virtual servers and data to an alternate cloud datacenter to provide failover coverage in the event of a man-made or natural catastrophe. We offer a number of flexible disaster recovery options to satisfy the most demanding government disaster recovery requirements and NIST Contingency Planning family of controls. Alternate cloud geographic zones are currently available in geographically separated U.S. cloud datacenters.

INTRUSION
DETECTION SERVICE

Managed Intrusion Detection Service

As a component of IT-CNP's Continuous Monitoring Program, our network-based intrusion detection system (IDS) monitors all network or system traffic for malicious activity or policy violations.

LOG AGGREGATION
SERVICE

Managed Log Aggregation Service

As a component of IT-CNP's Continuous Monitoring Program, our cloud log aggregation service collects and centralizes system logs from customer's virtual servers and stores them for a minimum of 30-month retention period.

VULNERABILITY
SCANNING SERVICE

Managed Vulnerability Scanning Service

As a component of IT-CNP's Continuous Monitoring Program, our Vulnerability Scanning Service includes a collection of industry's leading and custom vulnerability scanning tools to ensure periodic identification of customer server vulnerabilities and compliance benchmark configuration validation. The results are analyzed by IT-CNP's SOC personnel, recorded in customers' system-specific Plan of Actions and Milestones (POAM) tracking tool and distributed to the customer for review and resolution on monthly basis.

INCIDENT RESPONSE AND
TRACKING SERVICE

Managed Incident Response and Tracking Service

Our Incident Response and Tracking Service is fully compliant with NIST Special Publication 800-61 Revision 2 – Computer Security Incident Handling Guide, FedRAMP incident response guidelines and agency-specific tailored incident response procedures to ensure that every customer system has access to IT-CNP's SOC Computer Security Incident Response Capability (CSIRC).

CONTINUOUS MONITORING
SERVICE

Managed Continuous Monitoring Service

IT-CNP provides all the necessary tools and services to enable our cloud customers to fully comply with each federal government agency's demanding continuous monitoring requirements without excessive up-front budgetary investments.

CONFIGURATION
MANAGEMENT SERVICE

Configuration Management Service

IT-CNP provides the necessary tools and services to enable our cloud customers to fully comply with each federal government agency's configuration management requirements.

ASSET MANAGEMENT
SERVICE

Asset Management Service

Tracking and documentation of customer information system assets including network devices, servers, appliances and major installed components (e.g. databases). This service is critical for compliance with federal government continuous monitoring program requirements.

SYSTEM SECURITY
ASSESSMENT SERVICE

System Security Assessment Service

IT-CNP offers an option to perform system security assessment service based on customer security compliance framework to establish the current information security state and provide recommendations towards closure of any gaps identified during an assessment.



Digital Forensics Service

IT-CNP offers a number of digital forensics service options to accommodate the most demanding law enforcement forensic investigations and cyber defense analysis for computer related activities.



Assigned Information System Security Officer (ISSO)

IT-CNP provides a dedicated ISSO to your project. The ISSO is responsible for leading the preparation, coordination and ongoing maintenance of all required ATO paperwork to include the System Security Plan (SSP), Plan of Action & Milestones (POA&M), System Diagram and the System Inventory. The ISSO will also play a key role throughout the entire assessment and authorization process through maintaining close coordination with both the customer and Federal Client as needed.

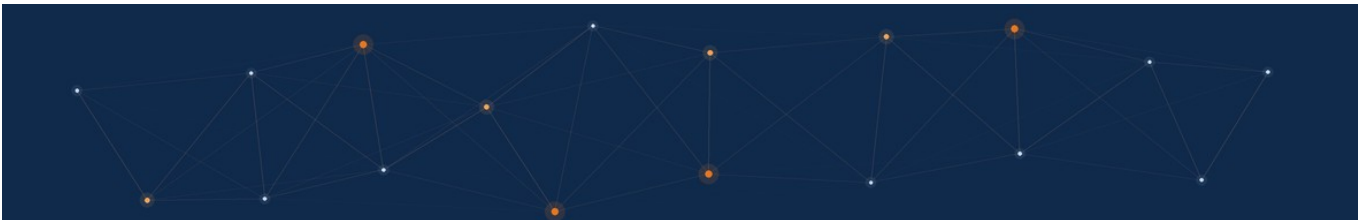
04

GOVDATAHOSTING CLOUD PLATFORM MANAGED SERVICES

Value-Added Services



SERVICE DESK
PORTAL SERVICE





ServiceDesk Portal Service

Our ServiceDesk Portal Service provides an electronic service request and change request tracking capability for IT-CNP's cloud customers. The service is configured for customer requestors to submit new service requests and initiate new change requests. Service requests include requests for additional resources, assistance in troubleshooting technical issues and reporting of technical malfunctions (incidents). IT-CNP tracks each request individually with emphasis of expedient request assignment for request resolution and high quality of service performed.



Software License Provisioning Service

IT-CNP provides a comprehensive software license provisioning service to ensure that customers can take advantage of leading software vendors' offerings and features approved for use by the government as a simple one-time fee or a fixed monthly fee.



Project Management Coordination Service

IT-CNP ensures that all new and existing customer system changes and major efforts and guided by an experienced project manager to ensure coordination between the technical and security compliance management teams.



System Design Service

IT-CNP technical engineering and security compliance personnel assist customers and federal/state government agencies in the design phase of their information systems in accordance with technical best practices combined with security compliance considerations unique to customer requirements and government agency guidance.



Cloud Readiness Assessment Service

As a cloud infrastructure provider, IT-CNP performs cloud readiness assessment services based on real-life enterprise government information system experience to ensure that customer stakeholders are provided with an actionable strategic report assessing their cloud migration readiness status.

05

GOVDATAHOSTING CLOUD PLATFORM MANAGED SERVICES

About Us



About GovDataHosting

GovDataHosting is a cloud division of IT-CNP, Inc.

GovDataHosting is a cloud division of IT-CNP, Inc., founded in 2001 and headquartered in Columbia, Maryland. We deliver FedRAMP High (Class D) Certified cloud infrastructure, security and compliance, technical support, and disaster recovery to federal agencies, state and local government, education and non-profit organizations, and government contractors.

Our single-source model bundles everything required to migrate to the cloud, achieve an agency-specific Authorization to Operate (ATO), and maintain continuous compliance — under one vendor, one contract, and one invoice. Customers inherit 300+ NIST 800-53 Rev 5 controls from our authorization boundary rather than building and assessing those controls themselves.

Services are delivered exclusively from U.S. cloud data centers in Columbia, MD; Cleveland, OH; and Dallas, TX, and are supported around the clock by our U.S.-based Security Operations Center staffed by U.S. citizens.

FedRAMP High (Class D) Certified · DoD IL2 Authorized · NIST 800-53 Rev 5 High · SOC 2 Type II · 24/7 U.S.-Based SOC · U.S. Cloud Data Centers Only

Solutions

Who we serve.

PUBLIC SECTOR

- ▶ **Civilian Agencies**
FedRAMP High (Class D) Certified hosting and continuous monitoring for civilian federal agency systems.
- ▶ **Defense Agencies (DoD)**
DoD RMF-aligned environments at IL2, with higher impact levels available through managed government cloud platforms.
- ▶ **State and Local Government**
Compliant hosting for state and local agencies, including CJIS-aligned environments.
- ▶ **Education / Non-Profit**
Cost-effective compliant hosting for education and non-profit missions, including managed Moodle.

GOVERNMENT CONTRACTORS

- ▶ **Prime Contractors**
Inherit our authorization boundary to meet agency security requirements on prime contracts.
- ▶ **Defense Contractors**
NIST 800-171 and CMMC-aligned enclaves for CUI and DFARS obligations.
- ▶ **Small Business (8(a)/SDVOSB)**
Compliance capability for small business set-aside contractors without in-house security staff.
- ▶ **FedRAMP SaaS Providers**
Build your SaaS on an inherited FedRAMP High (Class D) Certified boundary to accelerate your own authorization.

Platforms

Where your workloads run.

CLOUD PLATFORMS

- ▶ **Available Platforms**
Compare platform options and select the right fit for your workload and impact level.
- ▶ **GovDataHosting Cloud Platform**
Our own FedRAMP High (Class D) Certified infrastructure in U.S. cloud data centers.
- ▶ **AWS GovCloud Infrastructure**
Fully managed AWS GovCloud environments under our compliance and monitoring program.
- ▶ **Microsoft Azure Government**
Managed Azure Government environments for Microsoft-centric workloads.

CONTENT PLATFORM HOSTING

- ▶ **Drupal Hosting**
Managed Drupal core administration, patching, and hardening.
- ▶ **WordPress Hosting**
Managed WordPress hosting inside an authorized boundary.
- ▶ **Moodle Hosting**
Managed Moodle hosting for education and training programs.
- ▶ **Custom App Hosting**
Hosting and administration for custom and legacy applications.

Services

How we run them.

CLOUD MANAGEMENT

- ▶ **Fully Managed Platform**
We operate the full stack — infrastructure, operating system, security, compliance, and support.
- ▶ **Self-Service Platform**
Provision and manage your own resources on our compliant infrastructure.
- ▶ **Cloud Brokerage**
We procure, integrate, and manage third-party cloud services on your behalf.

SPECIALIZED SERVICES

- ▶ **Secure Cloud Enclaves**
Dedicated, logically isolated environments for CUI and other sensitive workloads.
- ▶ **Cloud AI**
Compliant AI and machine learning workloads inside an authorized boundary.
- ▶ **AI Fusion Lab**
An experimentation environment for government AI use cases.

Compliance & Contract Vehicles

COMPLIANCE FRAMEWORKS SUPPORTED

FISMA NIST 800-53 · FedRAMP · NIST 800-171 / CMMC · NIST CSF · DoD RMF (DoDI 8510.01) · CJIS

CONTRACT VEHICLES

GSA MAS · HHS BPA · Maryland CATS+

Talk to a federal cloud compliance specialist.

A Cloud Division of IT-CNP, Inc.

800-967-1004

www.govdatahosting.com

Columbia, Maryland