GOVDATAHOSTING

ADVANCED GOVERNMENT ORIENTED CLOUD HOSTING SOLUTIONS

SERVICE PORTFOLIO

FISMA CLOUD

SECURITY COMPLIANCE

DISASTER RECOVERY

APPLICATION SUPPORT

IT CNP Inc. | FedRAMP

FEDRAMP CERTIFIED CLOUD

Created to exclusively serve the demanding cloud hosting needs of Federal, state and local government agencies, GovDataHosting serves as a unique FISMA community and private cloud provider that delivers government compliant hosting, security compliance and hosting industry's best practices at a cost-effective price. GovDataHosting is a division of IT-CNP, Inc., a national provider of government-oriented IT operations, FISMA compliant cloud hosting, cyber security and IT logistics services.

UNIQUE DIFFERENTIATORS

GovDataHosting's mission is to continue as the market leader in FISMA compliant government cloud hosting solutions, as we seamlessly provide cutting edge security compliance options and pioneer more productive and cost-effective technologies that enhance our customers' security posture and fulfill our customers' cloud utilization mission goals.

- **Fully managed FISMA cloud hosting services**
- **Accelerated FISMA A&A approval path**
- **NIST & DIACAP compliant turn-key solutions**
- **Lower implementation risk**
- **Reduced FISMA A&A and operating costs**
- **PMI certified implementation management team**
- **U.S. based all U.S. citizen support team**
- **100% infrastructure availability SLA**
- **Responsive high priority enterprise support**
- **Active Portfolio of FISMA Compliant Customers**
- **Authorization To Operate (ATO) Guarantee**
- **Convenient fixed/consumption price models**
- **FedRAMP P-ATO moderate risk certified**

COMPLIANCE

GovDataHosting datacenters offer the hosting industry's maximum flexibility in choosing security compliance offerings available to U.S. customers.

FISMA   DIACAP   FedRAMP   National Institute of Standards and Technology

SUPPORT

Available 24/7/365, our customer support mission is to always provide responsive high quality support service and 100% customer satisfaction guarantee to all our customers regardless of their system size or budget.

We are proud to serve our customers with solutions that meet most challenging business, technical and system performance requirements while offering 100% availability and performance guarantee.

The expertise of our support team makes it possible to rapidly deploy your unique solution at our secure dedicated hosting datacenter at a fraction of the cost when compared with the cost of deploying the same solution within a Government facility.

DATACENTERS

Built to the hosting industry's best practices, all our datacenters feature multiple Internet access providers, precision environment, conditioned redundant power and facility security controls to accommodate government requirements.

All GovDataHosting Datacenters are located in the continental United States and supported only by U.S. Citizens.

Our network and all systems are continuously monitored to track system availability performance, uptime and security compliance (continuous monitoring). Our system monitors all solution components from bandwidth utilization to system connectivity and instantly alarms our customer service personnel to any service failure.

GovDataHosting maintains and guarantees the following metrics of availability for all components under IT-CNP management control as part of our cloud hosting Service Level Agreement (SLA):

- **100% Facility Infrastructure Guarantee**
- **100% Network Infrastructure Guarantee**
- **100% Hypervisor Server Infrastructure Guarantee**
- **100% Security Compliance Guarantee**

FISMA CLOUD

GovDataHosting Cloud Platform (GCP) is a FedRAMP certified multi-tenant community and private cloud platform that enables federal agencies and government contractors to procure virtualized server and network infrastructure components on a resource-specific basis available as a fixed price or consumption-based price models.

Building on a decade of providing FISMA compliant virtual hosting solutions, our FISMA Community Cloud is delivered as part of GovDataHosting Cloud Platform (GCP), a culmination of modern cloud web hosting technologies dedicated to supporting government defense and civilian agency information systems requiring National Institute of Standards and Technology Risk Management Framework (NISTRMF) Low and Moderate risk levels of protection. Service for High risk systems is also available for select agencies.

U.S. BASED DATACENTERS AND SUPPORT

Since GCP is a government oriented cloud solution, our service is only available to government agencies and government contractors hosting federal government data or other governmental entities wishing to follow federal government standards.

GCP platform datacenters are located within continental United States and supported by U.S. citizen personnel with positively adjudicated criminal background investigation and non-disclosure agreements signed upon hire.

All personnel providing support for customer systems undergo annual security awareness training.

FULLY MANAGED CLOUD INFRASTRUCTURE

GCP FISMA Community cloud offering is based on a fully managed Infrastructure as a Service (IaaS) model allowing customers control over their hosted

applications while GovDataHosting certified support personnel fully manages the underlying cloud and security infrastructure, hypervisor and operating system(s). As part of our fully managed cloud service for customers, GovDataHosting provisions and manages all cloud resources including network bandwidth, sufficient processing, disk and memory computing resources and rapid elasticity on an as-needed basis commensurate with budget and mission requirements.

This GCP IaaS offering is fully compliant with infrastructure related technical, operational and management controls referenced in NIST Special Publication 800-53 Revision 3 and Revision 4 documentation baselines, including additional FedRAMP tailored guidance.

GCP datacenter infrastructure leverages enterprise network and server hardware as the cloud physical layer infrastructure providing customers' virtual servers, processing and memory resources. Disk infrastructure is provided by enterprise storage platform equipped with FIPS 140-2 compliant self-encrypting disks providing encrypted storage for all government customer data at rest.

GCP offers a variety of virtual server operating systems for easy scaling while meeting all processing requirements and compliance with requisite NIST and FedRAMP standards.

BENEFITS OF GOVDATAHOSTING CLOUD

:: INNOVATION AND LEADERSHIP Dedicated to exclusively supporting U.S. federal, state and local government systems, GovDataHosting continues to pioneer new service offerings in providing GCP cloud customers unique solutions and compliance services. First to deliver a fully managed FISMA security compliance service and government oriented virtualized hosting platform, our customers benefit from GCP technology innovation, leadership and superior service delivery.

:: LOWER IMPLEMENTATION RISK GovDataHosting project management office, security compliance and technical personnel are uniquely trained and experienced in implementing complex mission critical government-oriented security compliant information systems, thus significantly reducing new cloud customer technical and security compliance implementation risk by leveraging and lessons learned from previous deployments and strong proactive management approach.

:: U.S. BASED DATACENTERS AND PERSONNEL 100% of GovDataHosting datacenters are located in the continental United States and all personnel undergo a criminal background check, while support personnel working with customer information systems and sensitive data also undergo a government sponsored background investigation. Hosting with GovDataHosting ensures that all customer data is kept within U.S. borders and that insider threat risk is minimized and continuously monitored.

:: REDUCED A&A AND CONTINUOUS MONITORING COST By leveraging direct experience with NIST and DIACAP based security process roadmaps and documentation templates, capitalizing on experienced implementation personnel, improving processes from prior successful implementation efforts and optimizing service delivery methodology, GovDataHosting significantly accelerates the initial A&A implementation cycle and delivers the required continuous monitoring support at reduced cost.

SYSTEM IMPLEMENTATION MANAGEMENT

Each customer system implementation within GCP infrastructure is directly planned and managed by GovDataHosting Project Management Office (PMO) comprised of Project Management Institute certified project managers specialized in government system implementation and security compliance to prevent common security compliance system deployment mistakes, minimize risks and provide strategic implementation and operational leadership resulting in enhanced system operational state and increased customer satisfaction.

IT-CNP assigns a technical project management lead to each new GCP cloud system deployment as a single point of contact, leadership, resource coordination and oversight for all technical implementation planning, as well as security compliance activities.

TECHNICAL & SECURITY COMPLIANCE SERVICES

GCP standard Infrastructure as a Service (IaaS) cloud offerings are complemented by our Beyond Compliance™ managed service offering, which includes comprehensive support for FISMA, NIST, DIACAP, FedRAMP and custom security compliance

requirements serving Executive, Legislative, and Judicial branches of the U.S. Government, as well as state and local government customers.

Beyond Compliance™ managed service enables GovDataHosting cloud customers to focus on their information system mission while having GovDataHosting security compliance managers and auditors perform security compliance tasking.

Our security compliance managed service ensures that necessary documentation required to establish the initial customer system authorization (A&A), as well as maintain the authorization through continuous monitoring is generated, retained and periodically provided to customer agencies to demonstrate on-gong system security compliance.

To augment or fully extend customers' internal resources, GCP has trained and certified personnel providing managed database, middleware, and COTS applications vended by Microsoft, Oracle, Red Hat, Apache, and other leading industry vendors, plus other supplemental services to meet customer-specific requirements.

Content Management System (CMS) support is also offered for Drupal and other content management systems.

SECURITY COMPLIANCE

As part of our FISMA/FedRAMP cloud offering for civilian and DoD federal agencies, GovDataHosting delivers a comprehensive Beyond Compliance™ managed security compliance service based on implemented operational, management and technical controls according to NIST Special Publication 800-53 Revision 3 – Recommended Security Controls for Federal Information Systems and Organizations, and NIST Special Publication 800-53 Revision 4 – Security and Privacy Controls for Federal Information Systems and Organizations. Our managed security compliance service is offered for systems categorized as low, moderate or high risk.

We understand how challenging and confusing government information system security compliance requirements may appear, which is precisely why GovDataHosting offers a comprehensive managed security compliance service allowing customers to focus on their information system's performance, purpose and mission.

Our Beyond Compliance™ managed security compliance service covers all necessary activities to configure and document each customer's information system in order to obtain an ATO, and continues with on-going continuous monitoring activities required to maintain accreditation.

Leveraging Beyond Compliance™ fully-managed service allows GovDataHosting Cloud Platform customers to focus on managing their hosted applications while GovDataHosting personnel provides complete management of all underlying technology and required compliance activities.

INITIAL A&A DOCUMENTATION PACKAGE

To prepare the initial A&A documentation package for each customer system, Beyond Compliance™ service includes full documentation of information system security compliance risk posture through documenting security compliance controls implemented, and preparing all the necessary artifacts to facilitate successful evaluation through the respective agency's Assessment and Authorization (A&A) process to subsequently obtain an Authorization To Operate (ATO).

A&A REQUIRED DOCUMENTS

:: **SYSTEM CATEGORIZATION**

:: **SYSTEM DESCRIPTION**

:: **SYSTEM BOUNDARY DIAGRAM**

:: **NETWORK DIAGRAM AND DATAFLOW**

:: **RISK ASSESSMENT**

:: **CONFIGURATION MANAGEMENT PLAN (CMP)**

:: **SYSTEM SECURITY PLAN (SSP)**

:: **SYSTEM CONTINGENCY PLAN (CP)**

:: **SECURITY TESTING AND EVALUATION (ST&E)**

:: **INCIDENT RESPONSE PLAN (IRP)**

CONTINUOUS MONITORING

Once authorized, it is critical for each information system to maintain its authorized security posture by performing required continuous monitoring activities.

Performing ongoing security assessments, as part of continuous monitoring, determines whether the set of implemented security controls in cloud hosted customer's information systems remains effective considering new vulnerabilities and exploits, as well as any planned and unplanned changes that may occur in the system and its authorized environment (authorization boundary) over time.

Security-related information collected through continuous monitoring is used to make recurring updates to the security assessment and authorization (A&A) package.

GovDataHosting ongoing due diligence and review of deployed security controls enables the security authorization documentation to remain current and allow its FISMA Cloud customers to make informed risk management decisions to enable maximum cloud service utilization.

By leveraging Beyond Compliance™ security compliance managed service for continuous monitoring, GovDataHosting FISMA Cloud customers are able to maintain ongoing awareness of their information security, vulnerability management status, and threats to support their organizational risk management decisions.

Our Information Security Continuous Monitoring service is delivered based on NIST Special Publication 800-137 – Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, as well as FedRAMP Continuous Monitoring Strategy & Guide.

Ongoing assessment of security controls results in greater transparency into the security posture of GovDataHosting FISMA Cloud platform customers and enables timely risk-management decisions.

OPERATIONAL VISIBILITY

An important security compliance management component of GovDataHosting continuous monitoring program is to provide evidence that demonstrates the efficiency of its program. At various intervals, GovDataHosting provides evidentiary information to FedRAMP as well as customer agencies in the form of artifacts and collaboration. Review of these deliverables allows agency authorizing officials to evaluate their system risk posture and report on compliance.

BENEFITS OF CONTINUOUS MONITORING

Information security management is recognized as a dynamic process that must effectively ensure confidentiality, integrity and availability of mission-critical processing assets and sensitive government data. GovDataHosting Beyond Compliance™ managed service enables FISMA cloud customers to identify and respond to new vulnerabilities, evolving threats and operational environment change. Utilizing Beyond Compliance™ continuous monitoring service results in:

- **Assurance of compliance with comprehensive NIST/FedRAMP ISCM requirements**
- **Continuous assessment and documentation of the required security controls and critical events**
- **Increased visibility into the security of cloud hosted assets and data protection processes**
- **Improved evaluation, authorization and control of changes to information systems and data**
- **Awareness and implementation of applicable threat, vulnerabilities and zero day exploits.**

GOVDATAHOSTING CONTINUOUS MONITORING

:: **VULNERABILITY MANAGEMENT**

:: **EVENT MANAGEMENT**

:: **MALWARE DETECTION**

:: **CONFIGURATION MANAGEMENT**

:: **INFORMATION MANAGEMENT**

:: **PATCH MANAGEMENT**

:: **INCIDENT MANAGEMENT**

:: **ASSET AND LICENSE MANAGEMENT**

:: **NETWORK MANAGEMENT**

:: **SOFTWARE ASSURANCE**

DISASTER RECOVERY

Our complete disaster recovery solutions ensure that your mission-critical systems are on-line and running despite unplanned interruptions to operations. Our unique methodology and technology enables Government customers to achieve cost-effective protection for their critical data. We will generate a unique recovery approach to meet your specific organizational and budgetary needs.

When you rely on GovDataHosting as part of your disaster recovery plan, you are always protected and prepared for the worst case scenario. To match the complex needs of Government business processes, we offer a variety of complete disaster recovery solutions for keeping you up and running despite unplanned technical or nature related business interruptions.

DISASTER RECOVERY BENEFITS

- **Cost-effective, expeditious resumption of business**
- **Expedited access to mission-critical data**
- **Significantly reduced exposure to risk**
- **Increased efficiency utilizing existing resources**
- **Peace of mind that your data is protected**

With our customized disaster recovery package, recovering your system is a quick, reliable and convenient process. Our engineering support integrates many decades of disaster recovery planning, design and disaster recovery best practices. When we assist you while recovering your data, our engineering support team will assign a recovery lead for your task to ensure a smooth and trouble-free data recovery until you are completely satisfied and all your data is back in the operational mode.

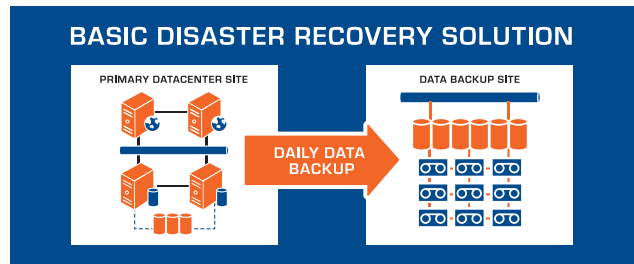## DISASTER RECOVERY CONFIGURATIONS

As part of our comprehensive disaster recovery strategy we offer a suite of scalable solutions that satisfy DIACAP, NIST, FISMA and other rigorous security policy requirements. GovDataHosting offers a set of standardized disaster recovery solutions, as well as customer-defined offerings. Our standard disaster recovery configurations are Basic, Enhanced and High-Availability. We can customize our disaster recovery configuration to your unique requirements, starting from one of our standard configurations.

BASIC DISASTER RECOVERY SOLUTION

Basic Disaster Recovery solution configuration accommodates customers that desire to have their data periodically backed up on a daily basis and securely transmitted to another facility for safe storage. The purpose of Data Backup Site is to

Basic Disaster Recovery solution configuration accommodates customers that desire to have their data periodically backed up on a daily basis and securely transmitted to another facility for safe storage. The purpose of Data Backup Site is to solely house backup data that can be used to restore service at another datacenter in case the primary datacenter site would become unavailable. This approach is commonly utilized for information systems that can sustain prolonged periods of downtime while service is being restored. All data is encrypted prior to being transmitted to the secure Data Backup Site.

BASIC DISASTER RECOVERY SOLUTION

PRIMARY DATACENTER SITE — DAILY DATA BACKUP — DATA BACKUP SITE

ENHANCED DISASTER RECOVERY SOLUTION

Enhanced Disaster Recovery solution configuration is designed to accommodate customers who are able to mitigate limited system downtime risk through periodic data backup to a Stand-By Site. This option is commonly utilized by security conscious organizations that are required to satisfy their disaster recovery needs with limited budgetary constraints. Enhanced Disaster Recovery solution is designed to restore service from another geographically dispersed datacenter facility within 4 hours of the primary datacenter site becoming unavailable due to a catastrophic event.

HIGH-AVAILABILITY DISASTER RECOVERY SOLUTION

High-Availability Disaster Recovery solution configuration is designed to provide fault-tolerant zero downtime service for mission critical information systems. Our most common approach to high-availability solution is to provide service concurrently from two separate sites (primary and alternate) while performing two-way replication of production data that ensures that information stays current in both environments.

APPLICATION SUPPORT

GovDataHosting provides a comprehensive set of application management options to augment each customer's system support team. While our technical team always manages the underlying operating system layer for each customer's virtual server, customers often request additional managed services for their database, middleware, COTS and customized applications.

Both options include database initial compliance configuration/hardening plus on-going continuous monitoring, patch and vulnerability management.

MICROSOFT APPLICATION SUPPORT OPTIONS

:: Microsoft Windows Server – Windows Server operating system management and support services are provided to all customers as part of our base cloud offering. Operating system support includes initial compliance configuration/hardening as well as on-going continuous monitoring, privileged user management, remote access management, patch and vulnerability management.

:: Microsoft SQL Server – SQL server database administration services are offered as a basic database administration service and advanced database administration service. Both options include database initial compliance configuration/hardening plus on-going continuous monitoring, patch and vulnerability management.

:: Microsoft Internet Information Services (IIS) – IIS web server administration services include web site setup and management, SSL certificate configuration, URL redirects, initial compliance configuration/ hardening and on-going continuous monitoring, security patching and vulnerability management.

:: Microsoft SharePoint – SharePoint farm administration services include basic farm setup, testing and on-going management. SharePoint farm administration support scope includes initial compliance configuration plus on-going continuous monitoring, SharePoint farm patch and vulnerability.

ORACLE APPLICATION SUPPORT OPTIONS

:: Oracle Database – Oracle database administration services are offered as a basic database administration service and advanced database administration service. Both options include database initial compliance configuration and hardening, plus on-going continuous monitoring, patch and vulnerability management.

:: MySQL Database – MySQL database administration services are offered as a basic database administration service and advanced database administration service.

RED HAT APPLICATION SUPPORT OPTIONS

:: Red Hat Enterprise Linux – Red Hat Enterprise Linux operating system management and support services are provided to all customers as part of our base cloud offering. Operating system support includes initial compliance configuration and hardening as well as on-going continuous monitoring, privileged user management, remote access management, patch and vulnerability management.

:: JBoss Web Server – JBoss web server administration services include web site setup and management, SSL certificate configuration, URL redirects, initial compliance configuration and hardening and on-going continuous monitoring, security patching and vulnerability management.

APACHE APPLICATION SUPPORT OPTIONS

:: Apache HTTP Server – Apache HTTP/Tomcat web server administration services include web site setup and management, SSL certificate configuration, URL redirects, initial compliance configuration and hardening and on-going continuous monitoring, security patching and vulnerability management.

CONTENT MANAGEMENT SYSTEM SUPPORT

:: Drupal CMS – Drupal core administration services include basic core setup, testing and on-going management. Drupal core administration support scope includes initial compliance configuration plus on-going continuous monitoring, Drupal core patch and vulnerability management. We also provides support for other content management systems (WordPress, Expression Engine, and Joomla)

CUSTOM APPLICATION SUPPORT

In addition to our standard application support options, GovDataHosting can provide support for hundreds of other specialized commercial and custom designed applications. Please contact us to discuss your specific application support requirements.

For Sales and Marketing Information Call us toll free at 800.967.1004

GOVDATAHOSTING

Created to exclusively serve the demanding cloud hosting needs of Federal, state and local government agencies, GovDataHosting serves as a unique FISMA community and private cloud provider that delivers government compliant hosting, security compliance and hosting industry's best practices at a cost-effective price.

GovDataHosting is a division of IT-CNP, Inc., a national provider of government-oriented IT infrastructure operations, FISMA compliant cloud hosting, cyber security and IT logistics services

CONTACT INFORMATION

Corporate Headquarters
9160 Red Branch Road
Columbia, MD 21045

Tel 410.884.1004
Fax 410.884.0412
U.S. Toll Free 800.967.1004

www.it-cnp.com
www.govdatahosting.com

IT CNP Inc.

FedRAMP
FedRAMP Certified Cloud

GSA Schedule
Contract GS-35F-099BA