MSP/Cloud Verify Report – Level 2

Report on Compliance with the MSPAlliance® Unified Certification Standard for Cloud and Managed Service Providers v.21

March 01, 2022 to February 28, 2023

Table of Contents

Section 1: Introduction 3

Section 2: Report by Management 6

Section 3: Independent Accountant's Report 8

Section 4: Description of the Cloud and Managed Services Environment 11

- Global Data Systems, Inc. Background 12
- Services Offered 12
- Services Verified Under MSPCV Report 14
- Events Subsequent to the MSPCV Period of Review 14
- External Service Providers Not in Scope of Report 14
- Explanation of the MSPCV Certification Table 14

Section 5: MSPCV Certification Table 16

- UCS Objective 01: Governance 17
- UCS Objective 02: Policies and Procedures 19
- UCS Objective 03: Confidentiality, Privacy, and Service Transparency 21
- UCS Objective 04: Change Management 23
- UCS Objective 05: Service Operations Management 25
- UCS Objective 06: Information Security 27
- UCS Objective 07: Data and Device Management 31
- UCS Objective 08: Physical Security 33
- UCS Objective 09: Billing and Reporting 35
- UCS Objective 10: Corporate Health 36

Section 6: Report Addenda 37

- SOC 2® Report Addendum 38

Table of Contents

Company Information ....Global.Data.Systems.........42

SECTION 1: INTRODUCTION

Dear Reader,

The following service provider has successfully completed the MSP/Cloud Verify Program® (MSPCV). The MSPCV is based on the Unified Certification Standard (UCS) for Cloud and Managed Service Providers® developed by the MSPAlliance®. For 20 years, the MSPAlliance has been promoting the cause of safe and secure outsourcing of IT management to managed service providers. One of the ways MSPAlliance accomplishes this goal is through the UCS.

The UCS consists of 10 control objectives and underlying controls that constitute crucial building blocks of a successful managed services (and cloud computing) organization.

UCS Objective 1: Governance
UCS Objective 2: Policies and Procedures
UCS Objective 3: Confidentiality, Privacy and Service Transparency
UCS Objective 4: Change Management
UCS Objective 5: Service Operations Management
UCS Objective 6: Information Security
UCS Objective 7: Data and Device Management
UCS Objective 8: Physical Security
UCS Objective 9: Billing & Reporting
UCS Objective 10: Corporate Health

During the MSP/Cloud Verify process, the provider is examined by an independent third-party public accounting firm and must demonstrate it has successfully met the applicable 10 control objectives and underlying controls and requirements. The MSPCV examination must be renewed annually.

There are two levels of examination under the MSPCV framework: Level 1, and Level 2.

Level 1 is a "point in time" examination. This means that the service provider met the necessary requirements as of the specified date of its examination.

A first-year Level 2 examination requires a minimum "period of review" of 3 months, while recurring Level 2 examinations typically cover a 12-month period of review. This means the third-party public accounting firm performed sampling and testing to verify that the objectives (and controls) were in place and operating effectively during the period of review.

This MSPCV report will describe each control objective, its purpose, and how the service provider has satisfied that control objective. While great care and detail went into the examination of the service provider, to protect the security of both the provider and its customers, some details of how the service provider delivers its services, including its security and privacy controls, are discussed here in general terms.

By using cloud computing and managed services from a verified provider, you are not only making a wise decision, but you are also helping to ensure that your service provider is abiding by the best practices and standards of a global community of service providers.

MSPAlliance Est. 2000
International Association of
Cloud and Managed Service Providers

Phone: 800-672-9205 | info@mspalliance.com | www.mspalliance.com

Thank you for helping us make the cloud computing and managed services community a safer place. If you have any questions about this examination report, you may contact your service provider. You may also request a call with the MSPAlliance and its examination team if you have specific questions about how the examination was conducted.

Signed,

MSPAlliance ®

Chapel Hill, North Carolina

SECTION 2: REPORT BY MANAGEMENT

310 Laser Lane, Lafayette, LA 70507
Tel 888.435.7986 - Fax 337.291.9739
getinfo@getgds.com

REPORT BY MANAGEMENT ON THE SERVICES ENVIRONMENT FOR THE MSP/CLOUD VERIFY PROGRAM™, BASED ON THE MSPALLIANCE UNIFIED CERTIFICATION STANDARDS FOR CLOUD AND MANAGED SERVICE PROVIDERS – LEVEL 2

May 12, 2023

We confirm, to the best of our knowledge and belief, that Global Data Systems, Inc. maintained effective controls over its Managed Services environment, referred to as its Cloud and Managed Services Environment, throughout the period March 01, 2022 to February 28, 2023. We provide reasonable assurance that Global Data Systems, Inc. has met, in respect to the MSP/Cloud Verify Program™, based on the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers v.21 – Level 2, requirements of the following objectives:

- Objective 1: Governance
- Objective 2: Policies and Procedures
- Objective 3: Confidentiality, Privacy, and Service Transparency
- Objective 4: Change Management
- Objective 5: Service Operations Management
- Objective 6: Information Security
- Objective 7: Data and Device Management
- Objective 8: Physical Security
- Objective 9: Billing and Reporting
- Objective 10: Corporate Health

The MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers is available at www.mspalliance.com/ucs. The UCS Objective Summaries and Purposes, along with Management's description of its procedures for compliance therewith, are included in the attached Global Data Systems, Inc. Description of the Cloud and Managed Services Environment.

Clements LeJeune
VP of Operations
Global Data Systems, Inc.
Lafayette, LA

SECTION 3: INDEPENDENT ACCOUNTANT’S REPORT

INDEPENDENT ACCOUNTANT'S REPORT

To the Management of Global Data Systems, Inc.
Lafayette, Louisiana

We have examined management of Global Data Systems, Inc.'s assertion that the requirements in respect to the MSPAlliance Cloud Verify Program based on the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers for the period of March 01, 2022 to February 28, 2023, is presented in accordance with respect to the MSPAlliance Cloud Verify Program based on the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers. Global Data Systems, Inc.'s management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

The information included in Objective 10: Corporate Health provided by Global Data Systems, Inc. is presented by Global Data Systems, Inc.'s management to provide additional information on the corporate health of the Global Data Systems, Inc. While Objective 10: Corporate Health is part of Global Data Systems, Inc.'s description of its Cloud and Managed Service Environment and the MSPCV Certification Table made available to user entities for the period March 01, 2022 to February 28, 2023, the information about Global Data Systems, Inc.'s Corporate Health has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

The information included in Section 6: Report Addenda provided by Global Data Systems, Inc. is presented by Global Data Systems, Inc.'s management to provide additional information and is not a part of Global Data Systems, Inc.'s description of its Cloud and Managed Service Environment or the MSPCV Certification Table made available to user entities during the period March 01, 2022 to February 28, 2023. Information about Global Data Systems, Inc., LLC's SOC 2® Report Addendum has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

Management asserts that Global Data Systems, Inc. has met the requirements of the MSP/Cloud Verify Program, based on the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers v.21 – Level 2, including the following objectives:

- Objective 1: Governance,
- Objective 2: Policies and Procedures,
- Objective 3: Confidentiality, Privacy, and Service Transparency
- Objective 4: Change Management,
- Objective 5: Service Operations Management,
- Objective 6: Information Security,

- Objective 7: Data and Device Management,
- Objective 8: Physical Security,
- Objective 9: Billing and Reporting, and
- Objective 10: Corporate Health.

In our opinion, management's assertion that, for the period of March 01, 2022 to February 28, 2023, Global Data Systems, Inc. has met the requirements in respect to the MSPAlliance Cloud Verify Program in accordance with the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers v.21 – Level 2, is fairly stated, in all material respects.

Bernard Robinson & Company, L.L.P.

BERNARD ROBINSON & COMPANY, L.L.P.
Greensboro, North Carolina
May 12, 2023

SECTION 4: DESCRIPTION OF THE CLOUD AND MANAGED SERVICES ENVIRONMENT

Global Data Systems, Inc. Background
Global Data Systems, Inc. is a full-service Managed IT company that, for more than 30 years, has helped people strategically grow their businesses by implementing first-class end-to-end IT services and solutions. Global Data Systems provides Managed Secured Connectivity, Voice and Collaboration, Managed IT, Security Services, and Cloud solutions for commercial Customers in the Healthcare Services, Oil and Gas, Marine Transportation, and Industrial Construction industries, but it's Global Data Systems' passion for Serving People and Making IT Simple that empowers Global Data Systems' Customers to reach their potential. You have enough to worry about, so Global Data Systems simplifies IT so you can focus on your business.

Global Data Systems is headquartered in Lafayette, LA, with additional offices and sales and technical personnel in Baton Rouge, LA, Lockport, LA, and Houston, TX.

Services Offered
Global Data Systems provides an alternative to the traditional on-premise IT teams and infrastructures. Global Data Systems also provides strategic planning and consulting to optimize Customer technology ecosystems. Global Data Systems provides the following:

IT Support and Helpdesk: Global Data Systems monitors and manages network and connected devices through its redundant Network Operation Centers (NOC) 24x7x365. The Global Data Systems team of solutions-specific engineers provides proactive management and alert resolution while delivering the highest Customer satisfaction ratings in the industry. Global Data Systems' IT support and helpdesk services are available in a model that fits a variety of business needs and budgets through the following:

- 24x7x365 United States (US)-based.
- On-Alert Support
- Onsite Support
- Remote Support
- US-based Helpdesk Tiers 1-3

IT Infrastructure: Global Data Systems provides turnkey solutions for IT infrastructure needs, from procuring and provisioning hardware and software to managing Customer maintenance and licensing contracts:

- Hardware Procurement
- Software Licensing
- Third-Party Vendor Management

Network Design & Architecture: Global Data Systems maintains and improves Customer network design and architecture, develops an IT roadmap, and delivers senior-level IT strategy through the following:

- Office365 Migrations
- Network Refresh
- Remote Site Implementations
- IMAC&D's
- IT Strategy Development

Managed Services: Global Data Systems provides a suite of managed services to support IT organizations and business stakeholders. From infrastructure and messaging to critical business applications, Global Data Systems works to make it easier to manage IT and deliver the technology that runs Customer businesses.

- Office365 Integrations
- Unified Email Management
- Managed Firewall and Antivirus
- Managed Data Center Infrastructure
- Managed Route/ Switch
- Managed Desktop
- Patches and Updates
- Managed Fax
- Email Spam Filtering

Managed Connectivity Services: Global Data Systems provides a suite of managed secured connectivity solutions. Whether it’s a corporate office, a branch office, or remote work sites, Global Data Systems has a secured connectivity solution to run Customers’ businesses.

- Managed Secured SD-WAN (NGC)
- Managed Secured Wireless Communications (NOMAD, NOMAD-2-GOM)
- Managed Secured Satellite Communications (NOMAD VOYAGER & NOMAD EXPLORER)
- Managed Mobility

Voice and Collaboration: Global Data Systems provides Customers with a full suite of voice and collaboration services to provide businesses with the necessary tools to operate their business from anywhere.

- nCONTACT™ Hosted VoIP
- Voice
- Voicemail
- Chat
- Meetings
- Video
- Collaboration
- Cloud Contact Center
- Managed SIP Trunking

Security: With an ever-changing threat vector and cyber criminals gaining sophistication daily, the need for Security Services has never been greater. Global Data Systems offers a full suite of security services to prevent, detect, and respond to threats in real time.

- Core Infrastructure Assessments
- Penetration Testing
- End-User Security Services
- Email Security Services
- Web Security Services
- Implementation Services
- On-Going Strategic Planning
- Multifactor Authentication

- Server Security
- Firewall Security
- Security Foundation Services
- Security Awareness Training

Cloud Services: Global Data Systems offers its Customers the ability to leverage world-class data centers and cloud platforms to provide the necessary secured compute and storage solutions that are necessary to operate business-critical applications.

- Core Infrastructure Assessments
- Colocation
- Private Cloud
- Infrastructure as a Service
- Hosted Desktop
- Local and Offsite Backup and Recovery

Services Verified Under MSPCV Report

This MSPCV report has been prepared to provide information on Global Data Systems' compliance with the MSPAlliance Unified Certification Standard v.21. The scope of this MSPCV report is on Global Data Systems' IT Support and Helpdesk, IT Infrastructure, Network Design and Architecture, Managed Services, Managed Connectivity Services, Voice and Collaboration, Security, and Cloud Services, and, in the context of the MSPCV report, Customers are defined as entities utilizing these services.

Events Subsequent to the MSPCV Period of Review

Through its membership in the MSPAlliance, Global Data Systems completed a System and Organization Control (SOC 2®) Type 2 Report subsequent to February 28th, 2023. Included in an appendix to this report, Global Data Systems has provided the mapping of the criteria reported on in its SOC 2® report to the UCS objectives and requirements utilized in this report.

External Service Providers Not in Scope of Report

Global Data Systems utilizes 3rd Party Data Destruction; and relies on the encryption controls and the data storage controls (physical security) of their cloud-based applications. Reference to the services provided by these sub-service providers is described in the applicable sections of this report. This examination did not extend to the policies and procedures of the sub-service providers utilized by Global Data Systems.

Explanation of the MSPCV Certification Table

In the following MSPCV Certification Table, Global Data Systems has disclosed its assertion of compliance with the Objectives and the underlying Requirements of the MSPAlliance Unified Certification Standard (UCS) for Cloud and Managed Service Providers v.21 - Level 2. Global Data Systems' assertion of compliance with the UCS Objectives and underlying Requirements is communicated through the use of the following symbols:

- √ - Overall compliance with the UCS Objective has been verified,
- ✓ - Global Data Systems asserts its compliance with the underlying Requirement,
- x - Global Data Systems asserts its compliance with the underlying Requirement is not fully met, or

- * - Global Data Systems asserts its compliance with the underlying Requirement is not applicable to either the services provided by Global Data Systems or is not within the scope of the examination.

As part of the MSPCV process, Global Data Systems is improving its controls and the underlying policies and procedures. While complete compliance with all Requirements is the goal of the examination, no system is perfect. Therefore, non-compliance with a minimal number of Requirements does not prevent overall compliance with the UCS Objective. For instances of noncompliance or a non-applicable Requirement, a summary is provided by Global Data Systems to communicate its mitigation of the root causes for noncompliance.

SECTION 5: MSPCV CERTIFICATION TABLE

UCS Objective 01: Governance

Summary and Purpose *The goal of the Governance Objective is to provide assurance to the Customer that the MSP has established a corporate and organizational structure designed to maximize efficiency, minimize risk, and provide sufficient oversight and accountability with regard to the services delivered. This objective also addresses external service provider management protocols of the MSP.*		✓
01.01	**Organizational Structure**	✓
01.02	**Strategic Planning**	✓
01.03	**Risk Assessments**	✓
01.04	**Software Licensing**	*
01.05	**External Service Provider Management**	✓

01.01: Organizational Structure

Global Data Systems has a two-member Owners group that is responsible for the strategic development and supervision of the company. The composition of the Owners group consists of a President and CTO. Each owner possesses some company stock.

Board of Directors meets quarterly. The agenda is published in advance and meeting minutes are retained by the Chairman of the Board, who serves as the Board Chair.

The Executive Team, except for the President, reports to the COO and meets weekly. The Executive Team members include the President, and CTO who are part of the governance structure. Additionally, the VP of Sales, Director of Finance, COO, Director of Human Resources and VP of Operations are part of the Executive team. EOS (Entrepreneurial Operating System) software is used to guide the meeting, provide structure, and document data and tasks.

FOCUS, chaired by the COO, consists of various department representatives. The mission of this committee is to facilitate communications throughout GDS, provide departmental perspective on all GDS projects, prioritize and define GDS projects and utilize GDS resources efficiently. The group evaluates PRF (Project Request Form) submissions, which may include new or revised Products or Services.

The FOCUS Project Administrator maintains project plans and detailed notes in a file-sharing platform for viewing by all GDS employees.

The GDS Operations team meets weekly to discuss tasks, to-dos, newsworthy company events, and ROCKS. The Change Management Committee meets each business day.

The organizational chart is updated as needed and is reviewed as part of the annual planning meeting agenda. The Executive team reviews the accountability chart annually, as part of their agenda.

The Global Data Systems’ organizational chart is maintained through an application that renders the chart from company directory information, which is updated upon every hire, separation, and organizational change. It is available to all company personnel within the company's associate portal intranet site. Changes to the organization chart (new hires, separations, and role or reporting changes) are communicated to the workforce through company-wide emails.

GDS has documented job descriptions and requirements for all positions. Requirements such as education and certificates are noted and listed in any job posting. Further, GDS utilizes a tier progression chart that lines out all requirements for engineers to advance through the GDS tier system.

01.02: Strategic Planning

The Executive Team led by the President is responsible for the company's strategic plans. The CTO is accountable for the engineering, documentation, and development of the plans. The Executive Team meets quarterly at which time the VTO is reviewed, updated if necessary, and approved by the Executive team members. Once archived using the EOS software, prior VTOs are available for review.

01.03: Risk Assessments

This activity is documented in their weekly meeting notes. In addition, the FOCUS team meets weekly and evaluates GDS risk in various financial, operational, and administrative areas. A risk assessment spreadsheet has been implemented as of January 2021 and is used to log and identify risks for each year.

01.04: Software Licensing

Global Data Systems asserts its compliance with the underlying Requirement is not applicable to either the services provided by Global Data Systems or is not within the scope of the examination.

01.05: External Service Provider Management

GDS has a documented Vendor Management Policy. Part of the policy is to identify the risk profile of all vendors and significant third parties based on business impact, Customer contact, contract term, and access to data. GDS evaluates Vendors with a Vendor Risk Analysis before they are on-boarded. An initial risk analysis should be conducted for each potential vendor by members of the Executive team. At a minimum, the risk analysis will utilize the Vendor Risk Rating Matrix to assign a Vendor Risk Rating of Low, Medium, or High risk. A vendor is assigned a risk rating based on the highest risk level attributable to the contract, or sum of all contracts, with that vendor. Exceptions to the assigned risk rating may be granted as noted by the Risk Rating Matrix.

UCS Objective 02: Policies and Procedures

Summary and Purpose *The goal of the Policies and Procedures Objective is to ensure the MSP has documented the necessary policies and procedures in order to maintain effective service delivery levels, as well as to minimize deviation from those established policies and procedures.*		√
02.01	**Documentation of Policies and Procedures**	√
02.02	**Data Breach and Cyber-Attack Policies and Procedures**	√
02.03	**Periodic Review and Approval**	√
02.04	**Internal Audit**	√
02.05	**Employee Acceptance**	√
02.06	**Training and Orientation**	√

02.01: Documentation of Policies and Procedures

Global Data Systems has an Employee Guidebook that covers the following topics:

- Building for the Future
- Mission
- Our Vision
- Our People
- Organizational Climate
- Quality
- Guidebook Purpose
- Employment
- Conduct and Behavior
- Compensation
- Benefits
- Health, Safety, and Security
- Workplace Guidelines
- Employment Separation

The following topics are addressed in the GDS Security Policy: Server Security, Network Security, Data Security, and Physical Security.

HR policies and procedures are maintained on a file-sharing platform, where they are available to employees. The review of these policies and procedures with new hires is tracked with a new hire checklist.

02.02: Data Breach and Cyber-Attack Policies and Procedures

The incident response policies in GDS' Cyber Security Incident Response Plan directly address cyber, and ransomware attacks, and provide incident response and communication services to any security breaches. GDS will formulate a response for Customers that are affected by the data breach and communicate the next steps to the appropriate Customer point of contact. GDS has procedures documented in the Cyber Security Incident Response Plan that cover the company's response and communication of the breach to the appropriate parties. However, it may differ from Customer to Customer; where appropriate. GDS has not made any ransomware payments within the past 12 months.

02.03: Periodic Review and Approval

Policies are reviewed annually, and meeting minutes are kept when changes are discussed. If a change is made the changes are tracked and approved before being published.

GDS management is responsible for the maintenance and administration of the Policies and Procedures Manual.

02.04a: Internal Audit

GDS performs an annual internal audit of its controls following a standardized checklist. This audit is tracked in a recurring ticket, and the completed checklist and remediations resulting from the audit are documented in the ticket notes. The scope and criteria of GDS' internal audit are documented in the internal audit checklist to guide the performance of the internal audit. VP Operations is responsible for reviewing and approving the internal audit report upon completion. This approval is documented. approved, and dated via DocuSign. Audit support documents and results are stored on an internal GDS repository referred to as Operations.

02.05: Employee Acceptance

New hires are required to sign acknowledgments for all policies as part of the new hire process. HR tracks the completion and signing of the acknowledgments in its standardized onboarding checklist. All the checklists reside within the employee file. GDS has an HRIS system that allows these to be automated and completed on an annual basis.

Updates to the Employee Handbook or specific policies are communicated to employees via email and all affected acknowledgments are re-signed. These acknowledgments are stored in each employee’s folder.

02.06: Training and Orientation

GDS has new hire training/orientation courses set up in the LMS (Learning Management System). These courses cover a variety of items. Once the initial training courses are complete, a new hire falls into the specific department training.

GDS has continuing training and education programs for employees. These are specific to each role, and position and may involve internal or self-study or external training by an external service provider. These are tracked by HR and normally supported by an education application form which allows for employees to be reimbursed for training or awarded financial compensation upon successful certification.

UCS Objective 03: Confidentiality, Privacy, and Service Transparency

Summary and Purpose *The goal of the Confidentiality, Privacy, and Service Transparency Objective is to ensure the MSP has sufficient policies and procedures related to the protection of Customer data, specifically protocols safeguarding confidentiality, privacy, and geolocation of managed data including external service provider-managed data.*		✓
03.01	**Employee Background Check**	✓
03.02	**Employee Confidentiality and Privacy Acceptance**	✓
03.03	**Data Classification and Encryption**	✓
03.04	**MSP Data Geolocation Disclosure**	✓
03.05	**External Service Provider Geolocation Disclosure**	✓
03.06	**External Service Provider Access Management**	✓
03.07	**External Service Provider Access Disclosure**	✓

03.01: Employee Background Check

All new hires are subject to background checks (7-year criminal history, SSN check, Motor Vehicle Report) and new-hire drug screening. The HR department orders and tracks the screenings and if a successful screening isn't acquired then the offer is rescinded.

03.02: Employee Confidentiality and Privacy Acceptance

The GDS Employee Agreement includes a Confidential and Proprietary Information section. All GDS employees are required to sign this Employee Agreement.

All GDS employees are required to sign and attest to their understanding and adherence to the company's confidentiality and privacy policies via the signing of an Employee Agreement and Employee Guidebook Acknowledgment as part of the new hire process.

03.03: Data Classification and Encryption

GDS has a Data Classification & Data Handling Document that contains Data Classifications and covers both internal and Customer data.

All data stored on Global Data Systems storage devices is encrypted at rest and in transit for Customers receiving backup services.

03.04: MSP Data Geolocation Disclosure

All Customer-stored data is housed in the GDS Datacenter located in Lafayette, LA except for the data associated with Customers who subscribe to our Geodiverse Secure Backup product. Customers are notified verbally in the sale process, and it is also noted in our Geodiverse Secure Backup Product Description.

03.05: External Service Provider Geolocation Disclosure

GDS Customers are made aware of where their Geo backups are located. For cloud infrastructure management the location is regional. Communication of this is verbal in the pre-sales process and Customers receive a Geodiverse Secure Backup Policy.

03.06: External Service Provider Access Management

Service Provider personnel receive temporary access only by request. Some Customers request that their vendor be granted access to GDS systems in this case GDS grants temporary access.

External service providers that request access to GDS or Customer systems are tracked within tickets. Management approves the access request. GDS does not currently monitor the third-party vendor's activities, however, access request tickets are only reviewed when requested by Customers.

03.07: External Service Provider Disclosure

Once third-party or vendor access is approved via request, GDS tracks the party access in a ticket. Customers are notified of third-party access via an automated email through the GDS ticket notification process. The email notification could go to a single requestor or a company distribution depending on how each individual Customer is configured.

UCS Objective 04: Change Management

Summary and Purpose

The goal of the Change Management Objective is to ensure the MSP has formalized change management policies and procedures that are under formalized change controls. Such change management documentation may include, if applicable, capacity planning, modification of MSP and Customer configurations, and patch management. Customer change management policies are documented based on the level of services delivered to the Customer by the MSP.

✓

04.01	**Configuration Documentation**	✓
04.02	**Service Level Categorization**	✓
04.03	**Internal Change Tracking**	✓
04.04	**Customer Change Tracking**	✓
04.05	**Capacity Planning**	✓
04.06	**Patch Management**	✓

04.01: Configuration Documentation

A standard onboarding MOP (Method of Procedure) is used for new managed services Customers. The checklist is followed as detailed in the MOP for initial onboarding. Then tickets are generated in the PSA to ensure consistent onboarding of assets and initiating service delivery.

The technical and procedural documentation for new Customers is stored within documentation software. This information is populated by manual entry and via automated synchronization with the RMM (Remote Monitoring and Management) tool. Information regarding Customer contacts and service types is documented within the PSA.

Service requests are funneled via the ticketing system/CRM. The client must submit an approval via quote signature. Completion is documented within a ticket created in the standard service deployment via playbooks and workflow. Customers can send in notification of cancellation via service ticket or by notification to the account manager. Tickets in the PSA will be used to track the removal of services.

04.02: Service Level Categorization

GDS uses a PSA tool to classify and identify all new, existing, and former Customers. Companies are identified by Name, Company Type, Industry, Agreement Status, and Agreement Types. Every active Customer has an agreement corresponding to the product or service to which they subscribe. All companies with an active Managed Service Agreement are given the status of active in the PSA. This allows Service Delivery to process requests for these Customers. GDS has four ticket priorities that drive different response and resolution goals by priority. These priorities apply to all Customers. GDS does not offer different priorities or SLAs by Customer.

Global Data Systems sets global SLA (Service Level Agreement) and priority standards across all Customers. Each Customer's profile denotes the Customer name, type of industry, the status of service eligibility, and type of Customer.

04.03: Internal Change Tracking

GDS has a documented Change Management Policy that outlines rules to be followed in the change management process. Employees can submit a request for a change as an internal change ticket, which is tracked as a Change Management ticket type. Once submitted, the change is reviewed during the daily Change Committee meeting, where committee members document the approval or rejection of the change. The implementation of the change is tracked in a new ticket or project, depending on the size and scope of the change. Internal Change requests are treated and handled as change management requests.

04.04: Customer Change Tracking

GDS uses a change management process for the request, approval, and processing of changes to Customer environments. These changes are tracked in PSA tickets. All Change Management tickets are reviewed by the GDS Change Management Board.

GDS tracks all Customer change requests in a Change Management PSA ticket. All Change Management tickets are reviewed by the GDS Change Management Board. Customer notification and approval are documented in these same tickets. Tickets include a MOP documenting the changes/steps being made.

GDS tracks all Customer change requests in a Change Management ticket. These changes are tracked in PSA tickets. All Change Management tickets are reviewed by the GDS Change Management Board. Customer notification and approval are documented in these PSA tickets.

04.05: Capacity Planning

GDS monitors both internal and Customer storage capacity and availability with an RMM tool. High consumption events trigger a service ticket, and the resolution can range from the removal of temporary files to providing additional storage through the change order process. Utilization is reviewed with Customers during the EBR process. GDS also monitors the aggregate storage available to Customers and is tracked on a weekly basis for capacity management.

GDS monitors their SAN (Storage Area Network) capacity continuously in a business intelligence reporting dashboard and reviews its SAN capacity on a weekly basis. The weekly review is tracked in GDS' Level 10 meeting standing agenda.

04.06: Patch Management

GDS provides Patch Management for their Customers on servers and workstations. GDS utilizes an RMM and PSA tool for patch management, testing, and logging. GDS has a Patch Management Policy to govern the delivery of these services.

Patches are tested internally prior to being applied. GDS has a test group, pilot group, and production group to organize patches. If a patch fails to apply in the testing phase an alert is automatically created to resolve the issue. If a patch causes an issue in the Customer environment, the Customer will submit a ticket. Tickets will also be automatically generated for devices that are not reporting patch data or are missing patches.

GDS has a standard standing maintenance window for non-mission critical server patches. For mission-critical servers, GDS coordinates with the Customer(s) and internal resources to perform patches during scheduled maintenance windows. The dates and times for server maintenance windows will vary by Customer and are documented in the RMM tool. The maintenance windows for workstations are followed by an ad hoc reboot notification that allows the Customer to reboot at the time of their choosing within 30 hours of the patch implementation.

Global Data Systems has a daily scan of accessible monitored/managed internal and Customer devices.

UCS Objective 05: Service Operations Management

Summary and Purpose *The goal of the Service Operations Management Objective deals with how the MSP identifies and responds to IT-related events that could impact services delivered to the Customer. In this UCS objective, the examination covers the MSP's Network Operations Center ("NOC"), Trouble Ticketing systems, and Service Desk operations specifically related to event management policies and procedures.*		✓
05.01	**Centralized Operations Center**	✓
05.02	**Support and Problem Logging**	✓
05.03	**Categorization and Correlation**	✓
05.04	**Support and Problem Resolution**	✓
05.05	**Operations Monitoring**	✓

05.01: Centralized Operations Center

The GDS Network Operations Center (NOC) & Service Desk are staffed by employee personnel to monitor, log, and resolve reported/identified problems, incidents, or service requests.

The GDS NOC is staffed 24/7/365 with additional on-call personnel for escalated support. The Service Desk's standard business hours are 7:00 am to 6:00 pm Central time Monday thru Friday (excluding holidays). Service Desk personnel are available on an on-call basis outside of standard business hours. The on-shift NOC employee will contact the appropriate NOC or Service On-Call representative via previously determined appropriate phone numbers.

05.02: Support and Problem Logging

Customer support issues/requests are logged in a PSA tool. Tickets are categorized and prioritized by source (email, RMM, phone, manual generation), Customer, and level of impact/urgency.

Tickets are automatically generated into the PSA from two RMM tools via email connector. Tickets are also automatically generated from backup applications to the RMM. GDS auto-closes tickets by Customer request from VSAT telecommunications Customers after a set period of time. GDS does not delete tickets. For these, tickets are logged, remain open for a prescribed amount of time, and, barring subsequent events, are auto-resolved.

GDS has service level targets based on the severity of the incident and its impact on the Customer. While the MSP typically tries to respond to all cases quickly, the SLA defines target response times for Customers (typically 15 minutes for Priority (P1) level cases, 30 minutes for Priority 2 (P2), 60 minutes for Priority 3 (P3), and 24 hours for Priority 4 (P4).

05.03: Categorization and Correlation

For monitoring generated tickets, the RMM tools provide info to the PSA that denotes priority. This priority level is predetermined upon the configuration of the monitored item/asset. GDS also utilizes a categorization list for each ticket that is generated. For phone or email-generated tickets, GDS has a documented process that is followed for proper ticket priority and categorization.

05.04: Support and Problem Resolution

GDS houses ticket documentation requirements in documentation software. Some Customers request modified documentation requirements, these modifications are stored in documentation software.

GDS has documented Customer communication in their NOC SOPs. This covers events identified in monitored environments. Updates, closures, and engineer assignments are auto communicated to the Customer from the PSA.

05.05: Operations Monitoring

Reviews are documented via a ticket which is automatically generated weekly. GDS reviews tickets SLAs weekly using reports. NOC/Service Desk Management performs the reviews and requests follow-ups where needed.

UCS Objective 06: Information Security

Summary and Purpose *The goal of the Information Security Objective is to ensure the MSP has implemented necessary controls to effectively govern access to managed data, networks, and systems that may compromise the security of both the MSP and the Customer. This includes remote access policies, user account administration, authentication, wireless access, segregation of duties, network security scans and assessments, and the monitoring of access to Customer systems.*		√
06.01	**Access to Applications and Environments**	√
06.02	**Super User and Administrator Access Security**	√
06.03	**Unique Users and Passwords**	√
06.04	**Revocation of Access**	√
06.05	**Strong Passwords**	√
06.06	**Segregation of Access**	√
06.07	**Periodic Review of Access Rights**	√
06.08	**Secure Remote Access**	√
06.09	**Network and Endpoint Security Management and Monitoring**	√
06.10	**Email Security**	√
06.11	**Antivirus**	√
06.12	**Wireless Network Security**	√
06.13	**Network Security Assessments**	√

06.01: Access to Applications and Environments

GDS has deployed RBAC (Role-Based Access Control) policies using AD to confirm personnel has network access based on defined roles and responsibilities by job role and GDS' security group's naming convention matches job roles for easy access. Access to GDS internal applications is also granted by the job role. Customer system and data access are restricted to GDS technical personnel by job role.

All service delivery systems are secured by AD and MFA.

When onboarding a new employee, a service ticket is created by the GDS HCM platform with the onboarding tasks listed as to-do items. Physical access and application access are determined by the RBAC title role assigned to the new employee. Employee, employee role, and access are documented in AD. When an employee changes roles, GDS HR sends a role change request to the support desk via email. A service ticket is created to track the work. The current RBAC role assigned to the employee is removed and the new RBAC role is applied in AD.

Requests for access not included in the assigned RBAC role must be approved by the employee's manager before being applied in AD.

All-access rights MACDs are reviewed through GDS change management.

06.02: Super User and Administrator Access Security

Access is controlled by RBAC policies in AD. Any modifications are approved through GDS change management. Default passwords for any application or device are changed to meet the GDS password policy. The passwords are documented in IAM/PAM (Identity Access Management/Privileged Access Management) software. Only designated IT resources can view or update the passwords.

06.03: Unique Users and Passwords

All GDS employees are given a unique username and password on the Active Directory Domain. Usernames are the employee's first name and last initial unless this is already in use by another employee. If this is the case, the employee is given a username that consists of the first initial and last name. Service accounts usually contain the name of the service and are unique.

Only certain groups have access to service accounts through role-based access. GDS enforces role-based access using RBAC policies in AD.

GDS does not have any guest/visitor accounts on its domain. GDS tech resources access Customer domains using unique accounts except where shared access is required by Customers.

Shared access accounts are secured by IAM/PAM based on RBAC policy.

06.04: Revocation of Access

GDS HCM creates a ticket with the offboarding tasks listed as to-do items. Access revocation is documented in the ticket.

06.05: Strong Passwords

GDS's password policy is a minimum of 10 characters, one upper case and one lower case letter, one number, and one special character. It must be changed every 90 days and employees are notified to change it. It cannot be reused within 24 passwords and the account will lockout after 10 failed attempts. Where applicable, GDS links the delivery services to AD, so that AD enforces the passwords. For applications not integrated with the AD, GDS enforces password policies to the extent possible. The passwords are enforced through the individual platforms and are documented in the platform by the manufacturer. For applications that have their own authentication and are not linked to AD, the user must use the corporate password policy when creating passwords. In the event the application password strength is greater than the corporate password strength, GDS employees use the application's password policy.

06.06: Segregation of Access

GDS segregation of duties is based on employee title. This is enforced by RBAC policies in Active Directory.

06.07: Periodic Review of Access Rights

Global Data Systems utilizes a recurring PSA ticket that has a set of tasks assigned to Global Data Systems Service Desk & NOC Managers and primary engineer to review user listings and access rights for internal applications, company intranet, data center logical/physical access, and active directory twice per year. The application owners and personnel enter their notes in the ticket, and it is reviewed by the Director of Operations & Infrastructure.

06.08: Secure Remote Access

GDS uses a VPN client, specific routes utilizing site-to-site VPN, or an RMM tool to access Customer networks.

Remote Desktop logs are kept on the server, and the RMM tool logs every time a user connects remotely. Logs are only reviewed if issues are reported through tickets.

06.09: Network and Endpoint Security Management and Monitoring

The GDS corporate network is protected by dual firewalls with network endpoint protection. The firewall provides an IPS (Intrusion Prevention System), web content filtering, and malware protection. Endpoint Protection protects the GDS corporate network and mobile users at the DNS layer. Email filtering software provides email filtering, spam, fishing, and virus protection for email. MFA software provides MFA for all corporate user access to desktops, laptops, and servers. It is also implemented on mission-critical applications and software. A SIEM (Security Information and Event Management) is used to gather security logs from across the enterprise. It is then configured to create alerts on malicious or concerning security activities. Another SIEM takes in SIEM data, threat intelligence, and other telemetry meaningful for security analysts. Playbooks are created to identify, investigate, and mitigate security threats found.

Endpoint protection continuously scans endpoints for malicious files and activity. Endpoint protection software protects GDS' corporate network at the DNS level from malicious traffic activity. All laptops have an endpoint protection roaming client that protects users off of the GDS network. MFA software protects against stolen credentials. SIEM agents monitor and gather endpoint logs that are sent to the SIEM for analysis.

All changes on the firewall are managed through change management tickets and change management board approval. All firewalls have been properly configured and their configurations are exported and backed up when a commit is made to the device, and they are backed up nightly.

Device health is managed through an RMM platform. All security logs and alerts are sent to the SIEM.

Security appliances, wireless switches, access points, and cradle points devices utilize a multitenant platform. Network appliances are managed on a Customer-by-Customer basis.

Firewall baseline configurations utilize security best practices. The Customer requested changes to follow the security best practices. Each Customer's fire configuration is customized to the Customer's specifications, with changes to the firewall configurations being handled and logged as part of the company's change management procedures. All firewalls have been properly configured and their configurations are exported and backed up as part of the nightly backup process. The health status of the firewalls is monitored in an RMM.

GDS provides SIEM as a service, but it can be wholly separated and independent from other service lines such as firewall management or monitoring services. Alerts/notifications about SIEM health are ingested in the ticketing system and generated cases that are addressed by SIEM Tier 1 support staff. Security alerts/events generated by SIEM solutions are also ingested into a dashboard and corresponding cases are generated and these are addressed, worked on, and enriched by the TA team.

06.10: Email Security

Email filtering software is utilized to monitor and protect emails internally by scanning incoming emails for potentially harmful links and attachments. In the event of blocked messages or stripped attachments, GDS users open a ticket with support for investigation Alerts are generated in the event of issues related to the delivery of the service. When applicable to the version sold under contract to a client the email filtering software is monitored for health and uptime.

When applicable to the version sold under contract to a client the email filtering software is monitored for health and uptime.

06.11: Antivirus

GDS uses two types of endpoint protection software to monitor all endpoints including laptops, desktops, and servers.

Based on the version of the product sold under contract emails are generated for notification of alerts.

06.12: Wireless Network Security

The company has implemented secured and managed wireless access points at the main office and branches which are protected by WPA2-Enterprise with PEAP (Protected Extensible Authentication Protocol) authentication using AD as an authentication source and identity governance software for device filtering/management.

Guest wireless connectivity is available and requires a pre-shared key that is provided to guests and employees to use on non-the company-owned devices. The guest wireless network is a segmented untrusted network that does not have access to the company's internal network and is segregated by firewall rules, only allowing traffic directly out to the internet.

06.13: Network Security Assessments

GDS performs a monthly vulnerability assessment of internal and external networks. The GDS security team reviews the monthly vulnerability report based on NIST (National Institute of Standards and Technology) best practices, industry threat intelligence, and known malicious CVE (Common Vulnerabilities and Exposures) from US-CERT. A ticket is generated each month for the activity. The Service Desk works to remediate those vulnerabilities that can be addressed. When issues are seen that SecOps considers to be a potential risk to GDS a FOCUS project is generated to discuss, evaluate corporate risk, and mitigate when directed. The company does not perform penetration tests at this time.

UCS Objective 07: Data and Device Management

Summary and Purpose *The goal of the Data Management Objective is to confirm the MSP has sufficient policies and procedures to ensure the integrity and availability of managed Customer and MSP internal data in the event of natural disasters, cyber-attacks (i.e., ransomware), and user error or malfeasance. This includes the implementation of data backup as well as encryption, security, retention, and restoration of managed Customer and MSP internal data.*		✓
07.01	**Customer Data Backup and Replication**	✓
07.02	**MSP Data Backup and Replication**	✓
07.03	**Data Recovery Testing**	✓
07.04	**Disaster and Business Continuity Planning**	✓
07.05	**Internal Data Destruction**	✓
07.06	**Customer Data Destruction**	*
07.07	**Device and Asset Management**	✓

07.01: Customer Data Backup and Replication

GDS contracts to provide backup and replication services to Customers. Each backup and replication policy is crafted to match the Customer's retention and backup requirements. These backup configurations are crafted during the Customer onboarding process. Changes to the backups are handled and tracked as part of the Change Management Process. This includes frequency for backups as well as retention time periods.

GDS encrypts the Customer's backup data while in transit and at rest. Per industry best practice GDS has instituted this as a standard as stated in their data classification policy.

Initial requirements are documented in the initial statement of work and subsequent changes are documented in Change Management tickets. Backups are automatically configured to encrypt while at rest & in transit within the backup/replication software.

07.02: MSP Data Backup and Replication

GDS utilizes the following standard for internal backups:

- Performs Daily Backups on all servers.
- Utilizes a 14-day retention policy for all backups.
- Currently performs an initial full backup and then reverse incremental via backup software's standard configuration on a nightly basis.
- The Internal Backup Policy covers all backups.

GDS encrypts internal backup data while in transit and at rest utilizing the functionality built into the backup/replication software.

07.03: Data Recovery Testing

Backup data restoration and recovery testing procedures are conducted for backup Customers on a bi-annual basis using scheduled backup/replication software backup jobs. The initiation and results of the testing procedures are documented in a PSA ticket.

07.04: Disaster and Business Continuity Planning

GDS has a Business Continuity Plan that is tested. We review the plan yearly and as we implement the plan during events requiring the plan to be placed into action, we perform analysis and update the plan during the next semi-annual meeting. The results of the test are documented in the minutes of the yearly meeting.

07.05: Internal Data Destruction

GDS has a documented internal data destruction policy that is located in GDS' SharePoint. Device destruction is tracked in PSA tickets.

07.06: Customer Data Destruction

Global Data Systems does not offer any Customer Data Destruction services.

07.07: Device and Asset Management

GDS has a documented BYOD and Device policy and it defines personal devices as any device not owned by GDS regardless of type. GDS manages and monitors all internal assets through their RMM. Only internal devices are loaded into this RMM by GDS. A list of all assets can be exported from this area of the RMM.

UCS Objective 08: Physical Security

Summary and Purpose *The goal of the Physical Security Objective is to ensure the MSP has documented policies and procedures governing the physical access and environmental security of the MSP's assets. MSP must demonstrate sufficient physical security controls at each facility, including controls such as physical access administration, card key, CCTV, on-site security, visitor/guest logs, and other effective security and environmental controls.*		✓
08.01	**Office Security**	✓
08.02	**Logging of Visitors**	✓
08.03	**Sensitive Area Security**	✓
08.04	**Revocation of Physical Access**	✓
08.05	**Data Center Special Requirement: Colocation**	✓
08.06	**Data Center Special Requirement: Environmental Controls**	✓
08.07	**Data Center Special Requirement: Maintenance**	✓

08.01: Office Security

GDS employs a variety of physical security controls to ensure the flow of personnel is secure. All exterior doors remain locked at all times and access to the facility is by electronic card scanners. Employees are assigned their own security cards during the onboarding process. The assignments of the GDS Access cards are managed and monitored in the access management system.

There are also some restricted areas within the facility that are accessible by approved employee security cards. There are a number of cameras throughout the exterior of the facility strategically placed to cover the various entry portals. The camera feeds are fed into the NOC, Field Services Manager, Procurement, and Warehouse offices.

Global Data Systems maintains the facility's security systems as a matter of daily business. If there are any issues with the systems, they are reported to facilities management immediately for repair or remediation. The remediation efforts are created and tracked in GDS' PSA ticket system.

08.02: Logging of Visitors

All non-GDS personnel must enter the facility through the reception area. The receptionist gathers the person's name and professional affiliation along with the time and date of entry to place into the Visitors logbook. They are issued a name tag with the info that they must display on their outerwear until they leave the facility. At this time the receptionist retrieves the badge and logs them out of the facility in the logbook.

08.03: Sensitive Area Security

GDS employs card scanners that control door locks that will allow access to approved personnel in restricted areas. These areas include the NOC, Secure Warehouse area, and Data Center. Personnel that require access to these areas go through the approval process upon hire. Approval is determined by the hiring manager and is managed and monitored via access management software. Any unapproved personnel needing access to these areas must be accompanied by the appropriate GDS employee at all times. GDS reviews access rights to sensitive areas and tracks them through quarterly tickets.

08.04: Revocation of Physical Access

As part of the GDS termination process, the security card is electronically disabled. The revocation is tracked in our ticketing system as well as the HR Employee Information management system.

08.05: Data Center Special Requirement: Colocation

GDS employs a Data Center Access/Security process that is documented in the Data Center Policy. The colocation services are provided in GDS' onsite Data Center. Access to the Data Center is physically restricted via security card-controlled door locks. Only approved employees have access to the Data Center. Customers are required to request access to the Data Center at least 24 hours in advance. Customers are required to update and maintain their access list with GDS. This information is kept in documentation software specific to the Customer account. When the Customer arrives at GDS they sign in through the receptionist post and are accompanied to the Data Center by a GDS employee.

08.06: Data Center Special Requirement: Environmental Controls

GDS has Smoke/Fire detectors monitored via a third-party monitoring platform. Waterless (FM200) Fire Suppression systems are also installed and inspected yearly. Redundant HVAC systems are monitored via an RMM tool and also alert if any water intrusion is seen under the raised floor. UPS systems are monitored via an RMM tool as are rack-mounted PDUs. There is also a generator panel within the NOC which indicates line power or generator power as well as the generator's health status using audible alerts. Datacenter temperature is monitored via environmental sensors which generate tickets automatically when conditions exceed configured thresholds.

08.07: Data Center Special Requirement: Maintenance

GDS has maintenance contracts with a third party for the UPS systems and another third party for the HVAC systems. The generator maintenance is performed by a third party.

UCS Objective 09: Billing and Reporting

Summary and Purpose *The goal of the Billing and Reporting Objective is to ensure the MSP is accurately monitoring service delivery, reporting, and invoicing for Customers in accordance with SLAs signed by both parties.*		✓
09.01	**Signed Contracts and Agreements**	✓
09.02	**Accuracy of Service Invoices**	✓
09.03	**Report Availability**	✓

09.01: Signed Contracts and Agreements

Service contracts for managed services relationships exist between both GDS and each Customer. These contracts are signed by both parties. GDS also uses a master service agreement in conjunction with its service agreements.

Each Customer signed proposal is countersigned by GDS. Each Customer must agree to an MSA prior to countersignature.

09.02: Accuracy of Service Invoices

Invoices are generated on the first of the month for recently completed work for recurring services and set-up fees. Pricing is dictated by the Customer's signed contract. Flat/fixed fee projects, like professional services, are billed upon completion. All out-of-scope work is billed per the standard rates.

09.03: Report Availability

Periodic reporting is established based on Customer requirements. GDS creates one or two sample reports from different reporting platforms to illustrate the capabilities of each during the Customer onboarding process. Once the Customer experiences the reporting and identifies a few use cases, GDS configures recurring reports (scheduled, and delivered by email) on their behalf. GDS will also perform a limited number of on-demand reports based on predefined manufacturer templates when a Customer requires an in-depth traffic review. GDS tracks report requests in a ticket.

UCS Objective 10: Corporate Health

Summary and Purpose *The goal of the Corporate Health Objective is to ensure sufficient corporate and financial health on the part of the MSP so that all of its Customers are adequately protected. Technical proficiency is only part of the MSP's value to the Customer. The MSP must be on firm financial footing, as well as risk-averse in a variety of areas unique to managed services and cloud in order to effectively deliver its services to the Customer.*		✓
10.01	**Operational Sustainability**	✓
10.02	**Significant Customer Risk**	X
10.03	**Gross Profit Margin of Services**	✓
10.04	**Customer Commitments**	✓
10.05	**Insurance**	✓
10.06	**Customer and Employee Retention Tracking**	X

10.01: Operational Sustainability

GDS was incorporated/formed in 1987 and has been providing services to Customers for over 35 years. As of the date of this report, GDS' financials showed that its operations were profitable over the previous 12 months. This profitability indicates operational sustainability and fiscal responsibility.

10.02: Significant Customer Risk

GDS' top five Customers represent approximately 71% of total GDS revenue, which is greater than the UCS best practice of 50% from the top five Customers. The largest GDS Customer represents only 24% of total GDS revenue which is greater than the UCS best practice of one Customer not representing more than 20% of total revenue.

10.03: Gross Profit Margin on Services

GDS maintains a gross profit margin on its services, which exceeds the UCS best practice of 30%. By exceeding the best practice, it shows that GDS is operationally efficient in its costs of delivering services.

10.04: Customer Commitments

The majority of GDS contracts have a term of 2 to 5 years. GDS utilizes month-to-month contracts on a limited basis, with those contracts supporting specific services or service lines.

10.05: Insurance

GDS carries insurance coverage commensurate with UCS best practices, including cybersecurity, errors and omissions, professional liability, and key man life.

10.06: Customer and Employee Retention Tracking

Over the last fiscal year, GDS has a managed services Customer retention rate of approximately 83% and an employee retention rate of 72%.

SECTION 6: REPORT ADDENDA

SOC 2® Report Addendum

Unified Certification Standard→ MSPAlliance® for Cloud and Managed Service Providers

FOR GLOBAL DATA SYSTEMS' SOC 2® MAPPING

This MSP/Cloud Verify Program™ (MSPCV) report for Global Data Systems Inc. (GDS) is based on the control objectives of the Unified Certification Standard for Cloud and Managed Service Providers (MSPs) (UCS) v.21. The UCS establishes best practices for MSPs in the delivery of their services to Customers. The UCS generally applies to most MSPs around the world, regardless of their vertical or market expertise and focus.

A Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) is a report that describes how a Service Organization meets the criteria defined in a set of Trust Services Criteria (TSCs)[1].

The following table represents the mapping of the GDS MSPCV report to their SOC 2® report[2]. This table was included in the issued and unqualified 2023 GDS SOC 2® Type 2 report on Security, Availability, and Confidentiality.

Trust Services for the Security, Availability, and Confidentiality Principles	**MSPAlliance UCS Objectives**									
	01	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**
CC 1.0 Common Criteria Related to Control Environments										
CC 1.1 The entity demonstrates a commitment to integrity and ethical values.	✓	✓	✓		✓					
CC 1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	✓									
CC 1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	✓									
CC 1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	✓	✓	✓							
CC 1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	✓	✓								
CC 2.0 Common Criteria Related to Communications and Information										

[1] TSC section 100, *Trust Service Criteria for Security, Availability, and Confidentiality, 2017* (AICPA, *Trust Services Criteria*)

[2] The TSC does not address the requirements of UCS Objective 9: Billing and Reporting and UCS Objective 10: Corporate Health.

CC 2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		✓	✓	✓	✓					
CC 2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	✓	✓	✓	✓	✓		✓	✓		
CC 2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.	✓		✓	✓				✓		
CC 3.0 Common Criteria Related to Risk Management										
CC 3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	✓		✓	✓						
CC 3.2 The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	✓		✓							
CC 3.3 The entity considers the potential for fraud in assessing risks to the achievement of objectives.	✓		✓	✓	✓					
CC 3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.	✓									
CC 4.0 Common Criteria Related to Monitoring Activities										
CC 4.1 The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	✓			✓						
CC 4.2 The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	✓	✓		✓		✓				
CC 5.0 Common Criteria Related to Control Activities										
CC 5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			✓	✓						
CC 5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.		✓	✓	✓						
CC 5.3 The entity deploys control activities through policies that establish what is expected and procedures that put policies into action.		✓		✓						
CC 6.0 Common Criteria Related to Logical and Physical Access Controls										
CC 6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	✓		✓	✓		✓	✓			

CC 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.					✓		✓			
CC 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.					✓					
CC 6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.							✓			
CC 6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.						✓				
CC 6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			✓		✓		✓			
CC 6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			✓		✓	✓				
CC 6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			✓		✓	✓				

CC 7.0 Common Criteria Related to System Operations

CC 7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			✓	✓	✓					
CC 7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		✓		✓		✓				
CC 7.3 The entity evaluates security events to determine whether they could or have resulted		✓		✓	✓	✓				

in a failure of the entity to meet its objectives (security incidents) and if so, takes actions to prevent or address such failures.										
CC 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		✓			✓					
CC 7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.					✓					
CC 8.0 Common Criteria Related to Change Management										
CC 8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.				✓		✓				
CC 9.0 Common Criteria Related to Risk Mitigation										
CC 9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	✓	✓		✓						
CC 9.2 The entity assesses and manages risks associated with vendors and business partners.	✓		✓							
A 1.0 Additional Criteria for Availability										
A 1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.				✓				✓		
A 1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.							✓			
A 1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.							✓			
C 1.0 Additional Criteria for Confidentiality										
C 1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		✓	✓				✓			
C 1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			✓				✓			

Trust Services Criteria Determined to be Not Applicable

The services provided by Global Data Systems, as described, address the common criteria related to security and the additional criteria related to availability and confidentiality, with the exception of the following

COMPANY INFORMATION

Examined Company:

Global Data Systems
310 Laser Lane
Lafayette, LA 70507
Phone: (337) 291-6500
www.getgds.com

Independent 3rd Party Auditor:

Bernard Robinson & Company
1501 Highwoods Blvd, Suite 300
Greensboro, NC 27410
Phone: (336) 294-4494
www.brccpa.com

Examining Body:

MSPAlliance®
Phone: 800-672-9205
www.mspalliance.com