MSP/Cloud Verify Report – Level 2

Report on Compliance with the MSPAlliance® Unified Certification Standard® for Cloud and Managed Service Providers v.2020

December 1, 2019, to November 30, 2020

Table of Contents

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 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.

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.

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

Phone: 800-672-9205 | 100 Europa Drive, Suite 569, Chapel Hill, NC 27517
www.mspalliance.com

SECTION 2: REPORT BY MANAGEMENT

MAINSTREAM TECHNOLOGIES

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

March 23, 2021

We confirm, to the best of our knowledge and belief, that Mainstream Technologies, Inc. maintained effective controls over its Managed Services environment, referred to as its Cloud and Managed Services Environment, throughout the period December 1, 2019 to November 30, 2020. We provide reasonable assurance that Mainstream Technologies, Inc. has met, in respect to the MSP/Cloud Verify Program^{TM}, based on the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers v.2020 – 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 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 Mainstream Technologies, Inc. Description of the Cloud and Managed Services Environment.

John Burgess, President
Mainstream Technologies, Inc.
Little Rock, Arkansas

SECTION 3: INDEPENDENT ACCOUNTANT'S REPORT

brc Bernard Robinson
& Company, L.L.P.

INDEPENDENT ACCOUNTANT'S REPORT

To: Management of Mainstream Technologies, Inc.
Little Rock, Arkansas

We have examined management of Mainstream Technologies, 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 December 1, 2019 to November 30, 2020, 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. Mainstream Technologies, 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 American Institute of Certified Public Accountants. 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.

The information included in Section 6: Report Addenda provided by Mainstream Technologies, Inc. is presented by Mainstream Technologies, Inc.'s management to provide additional information and is not a part of Mainstream Technologies, Inc.'s description of its Cloud and Managed Service Environment or the MSPCV Certification Table made available to user entities during the period December 1, 2019 to November 30, 2020. Information about Mainstream Technologies, 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 Mainstream Technologies, 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.2020 – 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 Management
- Objective 8: Physical Security
- Objective 9: Billing and Reporting
- Objective 10: Corporate Health

In our opinion, management's assertion that, for the period of December 01, 2019 to November 30, 2020, Mainstream Technologies, 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.2020 – Level 2, is fairly stated, in all material respects.

Bernard Robinson & Company, L.L.P.

BERNARD ROBINSON & COMPANY, L.L.P.
Greensboro, North Carolina
March 23, 2021

SECTION 4: DESCRIPTION OF THE CLOUD AND MANAGED SERVICES ENVIRONMENT

Mainstream Technologies Background

Mainstream provides Full-Service IT Support, Managed Hosting, Managed Virtual Hosting, Colocation, Disaster Recovery, Security Services, and Software Development services to Customers seeking to improve and secure their IT environments, while also decreasing costs. Mainstream delivers customized solutions for national and regional businesses and local and state governments through four distinct service lines:

Services Offered

Managed Hosting, Managed Virtual Hosting, and Colocation – Through its data center, Mainstream provides Customers Managed Hosting, Managed Virtual Hosting, and Colocation services. These services provided by Mainstream include, but are not limited to:

- Colocation
  - Secured rack or cage storage within the data center
  - Environmentally controlled and monitored areas
  - Redundant power and data connectivity
  - Ad hoc hourly "hands-on-site" IT support
  - Managed Hosting

- Colocation services in addition to:
  - Server management and administration
  - Hardware set up
  - Patch management
  - Backup management
  - System and network monitoring
  - Managed Virtual Hosting

- Mainstream-provided hardware in addition to:
  - Secured virtual server provisioning
  - Application hosting accessibility
  - Server management and administration
  - Patch management
  - Backup management including local and remote backups
  - System and network monitoring

- GetITback Disaster Recovery (DR) – Service offering that provides remote business continuity and disaster recovery to Customers that are outside the Mainstream datacenter. The service offering includes:
  - File and system level off-site backup services
  - Backup data set retention
  - System state backups
  - Secure transmission and storage of data

- Full-Service IT Support – Mainstream provides server, infrastructure, desktop, and end-user support services onsite and remotely to Customers. The support services include the assessment, planning, implementation, monitoring, and proactive maintenance of Customer systems by Mainstream personnel. This line of service is provided to ensure Customer maintained environments are configured to an acceptable standard while also supporting system availability.

- Managed Security Services – Mainstream provides cybersecurity services that include:
    - Managed Security Information and Event Management ("SIEM")
    - Managed File Integrity monitoring
    - Managed Active Directory integrity monitoring
    - Vulnerability scanning and management
    - Vulnerability remediation
    - Managed End-User Security Awareness Training
    - Infrastructure policy compliance scanning
    - Governance, Risk, and Compliance consulting

- Software Solutions – Mainstream employs a staff of programmers and developers to provide its Customers technology environmental solutions that will improve the efficiency and effectiveness of their business. This line of service includes, but is not limited to the following solutions:
    - Custom Software Design and Development
    - Lean Sourcing – Enhanced staff augmentation
    - IN-FLIGHT Consulting – Software project outsourced development
    - Agile SCRUM Rapid, Iterative Development
    - Business Process Analysis
    - Sunset Application Support
    - Collaborative Chief Technology Officer

Services Verified Under MSPCV Report
This MSPCV report has been prepared to provide information on Mainstream's compliance with the MSPAlliance Unified Certification Standard v.2020. The scope of this MSPCV report is on Mainstream's Full-Service IT, Managed Hosting, GetITback DR, and Managed Security 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, Mainstream completed a SOC 2 Type 2 Report after Dec. 1, 2020. Included in an appendix to this report, Mainstream 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
Mainstream utilizes subservice organizations for SIEM services, Electronic Visitor Logging, and Antivirus protection. Mainstream relies on the encryption controls and the physical security controls of the following cloud-based applications: the RMM, SIEM, backup applications, vulnerability scanning applications, electronic visitor log, documentation application, and the password vault. Reference to the services provided by these subservice providers are described in the applicable sections of this report. This examination did not extend to the policies and procedures of the subservice providers utilized by Mainstream.

Impact of COVID-19
During the year 2020, there have been considerable impacts in the United States, Europe and across the world arising from the coronavirus (COVID-19) pandemic and Government actions to reduce the spread of the virus. Mainstream also took appropriate actions as needed to protect the public health and that of its associates.

The Management of Mainstream believes that COVID-19 and the service organization’s response to it had no significant impacts to our internal controls. There have been no significant changes to the design, existence or operations of the specified internal controls as a result of COVID-19.

In addition, there have been no significant changes to our reporting responsibilities or complementary user entity controls as a result of COVID-19.

Explanation of the MSPCV Certification Table

In the following MSPCV Certification Table, Mainstream 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.2020 - Level 2. Mainstream's 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,
- ✓ - Mainstream asserts its compliance with the underlying Requirement,
- × - Mainstream asserts its compliance with the underlying Requirement is not fully met, or
- * - Mainstream asserts its compliance with the underlying Requirement does not apply to either the services provided by Mainstream or is not within the scope of the examination.

As part of the MSPCV process, Mainstream 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 Mainstream 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 assure the Customer that the MSP has established a corporate and organizational structure designed to maximize efficiency, minimize risk, provide sufficient oversight and accountability with regards 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

Mainstream has a five-member Board that is responsible for the strategic development and supervision of the company. The composition of the Board is as follows: Two representatives selected by each of the two co-plurality shareholders and one representative selected by the pool of remaining shareholders. Two of the five directors are external. The Executive Committee (XCOM) is responsible for the day-to-day operations of Mainstream. Executive Committee members are the Vice President of Information Technology, Vice President of Software Solutions, and the President.

Board meetings are held every 1-2 months (at least once per quarter), with agendas published to directors in advance and meeting minutes retained by the President, who serves as the Board Chair. XCOM meetings are held every 1-2 weeks, at least once a month, with meeting minutes retained by the President.

As part of its operations, Mainstream has the following committees that impact managed services operations:

Risk Assessment Committee: Charged with assessing the organization's awareness of and preparedness for known and emerging technological, financial, environmental, and legal risks to the organization, its workforce, and its Customers which exist due to the nature of the organization's activities. Members:

- President
- Vice President of Information Technology
- Director of Security Services
- Director of Research and Consulting
- Director of Information Technology

Information Security Committee: charged with maintaining the organization's policies and procedures regarding the protection of the information assets of the organization and customers of the organization relative to the needs of the organization, its customers, and relevant laws and regulations. Members:

- President
- Directory of Security Services
- Director of Research and Consulting
- Director of Information Technology

UCS Objective 01: Governance

IT Leadership: charged with overseeing managed services operations, customer infrastructure projects, and IT business development. Members:

- Vice President of Information Technology
- Director of Information Technology
- Director of IT Sales
- IT Senior Consulting Engineer

SEC Leadership: charged with overseeing managed security services operations, security consulting projects, and security business development. Members:

- President
- Director of Security Services
- Cybersecurity Relationships Manager
- Director of Marketing

The Risk Assessment Committee and Information Security Committee both meet on at least a monthly basis. The President retains meeting minutes for both committees. IT Leadership and SEC Leadership both meet weekly; minutes are not retained for these operational-nature groups.

An organizational chart documenting Mainstream's operational structure and reporting hierarchy is maintained by Human Resources. To ensure segregation of duties within the company, Mainstream has segregated its data center and managed services operations, software solutions operations, and cybersecurity operations into separate operational units, each of which is documented in the company organizational chart.

The Mainstream 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.

The responsibilities for the members of XCOM as well as the personnel within the organization are documented on the second page of the organizational chart. The responsibilities are documented to show the management and daily operations duties for which each position is responsible. Executive Committee members, the Director of Information Technology, and the Director of Security Services have the educational experience as well as technical and administrative expertise developed over lengthy careers both before and during their tenure with Mainstream to perform their assigned duties.

01.02: Strategic Planning

Mainstream maintains a Strategic Plan and conducts a continuous strategic planning process. Input is requested bi-annually from Mainstream's workforce, vendors, customers, and select independent parties regarding trends both internal and external to Mainstream which could affect Mainstream's strategic position. Reported trends are tracked and assessed by the XCOM and ad-hoc working groups comprised of the company's Senior Leaders (SL), depending on the scope and relevance of a particular issue. Proposed changes to Mainstream's Business Model to address relevant trends are developed by the ad-hoc working groups and forwarded to XCOM for approval and implementation. Strategic plans and priorities are set by XCOM and communicated to the Board annually via a presentation of the plans and statuses.

UCS Objective 01: Governance

01.03: Risk Assessments

An annual risk assessment is performed to identify internal and external risks to Mainstream. The risk assessment process is topical, with the assessment procedures being integrated with industry guidance to address identified risks.

The risk assessment process is overseen by the Risk Assessment Committee, with the Risk Assessment Committee meetings typically concluded for the year following the finalization of the risk assessment.

01.04: Software Licensing

Mainstream offers IaaS and other software licensing services. Mainstream owns the hardware and the virtualization software licenses, including the end-user licenses, typically managed under Mainstream's software suite SPLA and server management (VSPP).

The Director of Information Technology is responsible for completing the licensing calculation based on usage; the reporting process, usage meter, reporting reminder. The calculation spreadsheet is updated as needed. The reporting to both the software suite application and the backup/replication application is conducted on an on-demand basis, with the VP of Information Technology communicating the licensing to the Director of Information Technology upon notice. The VP of Information Technology is responsible for managing and reviewing the service provider licensing agreements for Mainstream.

01.05: External Service Provider Management

The Mainstream Information Security Policy (section XIX) defines the policies and requirements of evaluating and approving external service providers. External service provider due diligence is performed in the context of a risk assessment with approved external service providers being classified as critical or non-critical. Critical external service providers must submit to either individual background checks or provide preferably independent audit results, or sufficient documentation to allow oversight of their controls at a minimum, relative to the services or products utilized by Mainstream.

External service providers are initially assessed, approved, and identified as being critical or not by the Risk Assessment Committee before any system or information access is granted. Existing service providers who are deemed critical are evaluated annually by the Risk Assessment Committee; evaluation procedures consist of the reading and analysis of audit reports from those external service providers deemed to have a significant impact on the Company.

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 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	**Employee Acceptance**	✓
02.05	**Training and Orientation**	✓

02.01: Documentation of Policies and Procedures

General terms of employment, including confidentiality, work product ownership, compensation, and leave policies are covered in a standard employment agreement between Mainstream and each employee. Additionally, general policies, information, and HR procedures regarding an equal employment opportunity, non-harassment, FMLA, workmen's compensation, payroll, parking, travel and expense reporting, general office etiquette, and frequently asked questions and forms about employee benefits are stored on the company intranet site. Mainstream's Information Security Policy, also available on the company intranet, documents employment policies related to physical security, approved technologies, and acceptable use of company technologies.

Mainstream has documented Managed Services policies and procedures contained in a Service Operations Manual to communicate the security and control requirements for the daily operations of the Managed Services operations. All company policies and procedures are published on Mainstream's intranet site.

02.02: Data Breach and Cyber-Attack Policies and Procedures

Mainstream's Information Security Policy addresses incident response requirements and Mainstream maintains an Incident Response Plan which identifies roles and individuals responsible for cyber incident response activities and documents procedures to be followed in the event of cyber incidents, including breaches, which may occur in either Mainstream's internal environment or in the environments of Customers for whom Mainstream provides service. Mainstream is not bound internally by any specific regulations regarding data breaches but requirements for specific regulations that may apply in certain scenarios involving Customer environments are documented in the Incident Response Plan.

Mainstream provides services to Customers with differing requirements, whether internally determined or required by some applicable regulatory framework, for notifications regarding security incidents. Mainstream's Incident Response Plan documents the appropriate parties and communication requirements and responsibilities to those parties for data breach malicious software (ransomware), and cyber-attack scenarios where the communication and notification requirements differ. Upon detection of a security incident, any actions or communications performed will be documented in one or more service tickets associated with the event. Mainstream has not made any ransomware payments in the past 12 months.

02.03: Periodic Review and Approval

The Information Security Committee meets weekly throughout the year and reviews each section of the Information Security Policy twice during the course of a year, per the policy's requirement. Operational procedures are reviewed continually by the Managed Services leadership and are changed to address policy changes, product or solution changes, and observed service quality or efficiency issues.

Changes to the policy are packaged into periodic version updates to the policy with accompanying release notes summarizing changes from the previous version. All Mainstream associates must review and acknowledge receipt and understanding of each new policy version.

The Information Security Committee is responsible for reviews and updates to the policy. Recommended policy changes are submitted by the Information Security Committee to the Executive Committee for approval. Changes approved by the Executive Committee are then reported annually to the Board of Directors. Policy reviews and updates are tracked in the meeting minutes of the Information Security Committee. Review and approval of the policy by the Executive Committee and Board of Directors are documented in the meeting minutes of each body, respectively. Previous versions of the policy and release notes summarizing changes between versions are retained by the Information Security Committee.

02.04: Employee Acceptance

Each employee must sign his/her Employment Agreement and are introduced to the policy and procedure section of the company intranet as part of the new employee onboarding process. Upon hire, each employee must complete a training course on the Information Security Policy and must acknowledge receipt of the policy and agree to abide by the terms of the policy. Every employee must complete the policy training annually and each employee's progress and completion of the annual training is monitored and reported to the Executive Committee. Since Mainstream performs services with multiple Customers in the healthcare industry and is bound by multiple Business Associate Agreements, Mainstream has developed a HIPAA policy, also available on the company intranet, which each employee must read and agree to follow upon hire.

Updates to policies are communicated to employees during presentations at quarterly Company Meetings and company-wide emails. Current policy documents are available for review on the company's intranet site and the policy training portal. Associate acknowledgments of receipt and understanding of policy changes are tracked via an internal application.

02.05: Training and Orientation

Mainstream has a formal onboarding program for new hires that are tracked within the PSA onboarding ticket and is guided by the Service Operations Manual. Mainstream's Information Security policy is distributed to every new employee and they are required to complete Mainstream's Information Security computer-based training program. The Service Operations Manual is distributed to each new employee in the IT division upon hire.

Mainstream maintains employee-specific spreadsheets that define skill levels and identifies areas in which training may be needed. Continuing education goals are customized to the individual employee and are managed by the Director of IT Services and Director of Security Services to ensure they align with company goals and certification needs. Mainstream also tracks employee training in their training application.

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 the 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 Access Management**	✓
03.06	**External Service Provider Access Disclosure**	✓
03.07	**External Service Provider Geolocation Disclosure**	✓

03.01: Employee Background Check

Background checks are performed through Arkansas state police for misdemeanors and felonies. An FBI check, SSN, and OFAC check are also performed for anyone that will have access to the data center. Background checks are also conducted on existing employees by Customer request and are tracked by XCOM via a date record of the most recent background check performed on each employee. Any cases involving exception information encountered in the background check process are reviewed with the XCOM by the Chief Security Officer.

03.02: Employee Confidentiality and Privacy Acceptance

Confidentiality of company and Customer data is addressed in the employment agreement of each Mainstream employee and through Mainstream's Information Security Policy. Confidentiality and privacy policies are enforced through a combination of training and a role-based access control system which limits access to company and customer data to only those employees with a business justification. Mainstream addresses access and handling of Customer data that falls under specific regulatory requirements through separate policy documents specific to each Customer's requirements. Due to the extent of Mainstream's work in the healthcare industry, Mainstream has a documented HIPAA Policy to define the confidentiality and privacy requirements as they relate to Business Associates and data.

Employees are required to sign and attest to their understanding and adherence to Mainstream's confidentiality and privacy policies during the new hire process by signing the Employee Agreement, by signing an acknowledgment to attest their understanding of Mainstream's Information Security Policy, upon hire and for each revision to the Information Security Policy, and by signing a HIPAA Policy acknowledgment to attest to their understanding and adherence of Business Associate agreements and the associated data.

03.03: Data Classification and Encryption

Mainstream utilizes a six-tier data classification system, documented within the Information Security Policy, which provides for the following classes:

- Public
- Restricted (limited to Mainstream employees and certain Customers)
- Proprietary (limited to Mainstream personnel)
- Confidential (limited to a subset of Mainstream personnel)

UCS Objective 03: Confidentiality, Privacy, and Service Transparency

- Client Confidential (data belonging to a Customer which is limited to a relevant subset of Mainstream personnel)
- Regulated Client Information (data belonging to a Customer that falls under a formal regulatory framework (e.g., HIPAA, PIC, CJIS, etc.)

Backup data managed and hosted by Mainstream is encrypted in-transit between the Customer's environment and remote backup locations. Customers utilizing the GetITback DR Service are also encrypted at rest in a remote location. Mainstream stores the encryption passphrases for GetITBack DR Customer backups within the documentation. Mobile devices use OS-level encryption to encrypt the device drive with the unlock key stored in Active Directory.

03.04: MSP Data Geolocation Disclosure

Customers receive an annual disclosure via email regarding the location of Customer Data in the custody of Mainstream and any external service providers. With the request, the disclosure of data geolocation is handled/responded to by designated Mainstream personnel with knowledge of the information.

03.05: External Service Provider Access Management

External service providers do not have continuous access to Customer systems as part of Mainstream's standard service offerings. Mainstream's Information Security Policy states that contractors are granted access based on least privilege and removed once that access is no longer needed.

If a contractor or other external service provider needs access to Mainstream or Customer systems, access is documented for the request, provisioning, and removal in a ticket. Access is granted for the duration of the engagement. Upon project completion or other resolution of the need for access, the external access is revoked. Additionally, access to systems by contractors and external service providers is reviewed quarterly with a template ticket. The list of external access privileges is reviewed to ensure that access is still warranted for each case.

03.06: External Service Provider Disclosure

If an external service provider is utilized, this is documented in a ticket. If the provider is needed for a Customer system, approval from the Customer's designated point of contact is obtained in the ticket. This process is documented in the Information Security Policy. The potential use of external service providers is also disclosed in the Customer's contract.

03.07: External Service Provider Geolocation Disclosure

Customers receive an annual disclosure via email regarding the location of Customer Data in the custody of Mainstream and any external service providers. The Mainstream Information Security Policy and Procedures manual have been implemented to govern the identification and disclosure of the geo-location of third-party managed data.

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, the capacity planning, modification of MSP and Customer configurations, capacity planning, 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	**Customer Categorization**	✓
04.03	**Change Tracking**	✓
04.04	**Capacity Planning**	✓
04.05	**Patch Management**	✓

04.01: Configuration Documentation

Mainstream utilizes standard onboarding ticket templates for new managed services Customers. The tickets and tasks listed in the tickets are followed to ensure consistent onboarding of assets and initiating service delivery. Mainstream utilizes setup tickets for new SEC services Customers and does not capture Customer configuration data.

The technical and procedural documentation for new Customers is stored within the documentation application. This information is populated by manual entry and via automated synchronization with the RMM. Information regarding Customer contacts and service types are documented within the ticketing system.

Once a Customer notifies Mainstream of their desire to add or remove services, the Account Management Team is responsible for initiating and completing the contractual changes if any apply. Currently, products and services, stated on our websites that are referenced in the contracts can be applied with no contract changes or acknowledgment by the customer. The contractual changes, if any apply, are processed through either updating of the original agreement or the approval of termination of services notice. Once the contractual changes have been completed by the Account Management Team, a ticket is created to onboard or offboard the services.

Any change to services requires formal approval by the designated Customer contact. This approval is recorded as a contract addendum if it requires a contract change. If the service is already covered by the existing contract, then the request can be made and approved with a ticket. Products and services specified in the contract do not require contractual changes but are tracked in a ticket with approval.

04.02: Customer Categorization

Customers are categorized and identified within the ticketing system by company type, status, and agreements with corresponding SLAs. Agreements in the ticketing system are directly configured based on customer contracts.

04.03: Change Tracking

Modifications to Customer and internal configurations are documented in a ticket to ensure changes are evaluated and approved by an authorized point of contact (technical or financial contact) per the Customer's change management policies. Configuration data within the RMM (or any other ancillary application) is updated following implementation to accurately reflect the current Customer configuration.

UCS Objective 04: Change Management

Both Customer and internal change requests and approvals are logged within a ticket. Depending on the nature of the issue or change request, the ticket may be escalated to the appropriate Customer point of contact to approve the request. This point of contact is defined within the ticketing system. Once the change is made it will be logged in the ticket and the ticket will be marked with a completed status.

04.04: Capacity Planning

Storage capacity is monitored through the RMM with 2-stage alerts that are based on thresholds set within those monitors. When a threshold is reached, a ticket is created by the system and assigned to an engineer. Any storage capacity issue that poses a risk to production availability is worked according to its pre-defined priority. If the problem can be mitigated with software or data usage changes, those changes are communicated through tickets and executed in a manner consistent with Customer expectations (approval and/or remediation). If a hardware change is required, Mainstream will prepare a specific recommendation for the Customer to approve and/or purchase. Storage Capacity planning is primarily done manually through Mainstream's periodic review process (at least annually) and is used as a factor in planning future upgrades and replacements. This process is tracked in the periodic infrastructure review ticket.

04.05: Patch Management

Mainstream's patch management policies and procedures reside in the Information Security Policy and govern the application of patches applied in maintenance tickets. Monthly maintenance tickets are auto generated based on a ticket template. The ticket template is configured to notify a designated Customer contact of their maintenance (or patch) schedule. If the scheduled maintenance window needs to be adjusted, the designated Customer contact may contact Mainstream to reschedule the maintenance window. If no communication is received from the Customer, the maintenance will be performed. Patching is identified, applied, and logged by patching tools where applicable.

Patches are applied during a regularly scheduled maintenance window, with patch notifications issued before this window. These notifications communicate the extent of the patch and maintenance window to Customers and are sent the morning before the maintenance window. This notification is generated by the Maintenance ticket. Maintenance windows are mutually agreed upon during the new customer onboarding process, with a standard maintenance window schedule. However, if the Customer has specific requirements regarding the maintenance windows and patch testing, then those requirements are communicated during onboarding and documented in their ticket template. Once the patches have been applied and the production status of the systems restored and verified (according to the monthly maintenance documentation), then a ticket update is sent to the Customer contact to communicate that maintenance has been completed.

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 Mainstream IT Service Network Operations Center (NOC) and Support center are staffed by personnel to monitor, log and respond/resolve reported/identified problems or incidents from 8 am to 5 pm Central time Monday thru Friday. The NOC is located within Mainstream's Little Rock location and also serves as security and escort for the Mainstream datacenter. After hours critical alerts are sent via an SMS/text to an on-call engineer for resolution. After-hours phone calls are received by a calling service that then follows a calling tree to reach a mainstream engineer. The calling service does not have access to Mainstream's systems.

Mainstream IT Service has a defined schedule for dispatch and engineer staff to cover the published hours of operation. Emergency/after-hours on-call is a set schedule and rotated between the engineers weekly. This schedule is maintained by a designated Sr. Engineer in a ticket.

05.02: Support and Problem Logging

Customer support issues are handled through the ticketing system. Issues may be called into the dispatcher who then creates the ticket or emailed directly to the ticket system from the Customer. All new tickets are triaged by the dispatcher and assigned metadata that includes the contract agreement, type, and subtype of the issue for categorization. Priority may be assigned based on the number of people affected and the business impact on the Customer.

NOC alerts are created from the monitoring systems and automatically create tickets in the ticketing system. The interface for the ticket creation is dependent on the monitoring system and includes a two-way API and inbound email connector. Non-critical NOC tickets are dispatched by the dispatcher to the engineers. Critical NOC tickets will additionally send SMS/text to the on-call engineer 24x7 to make sure that the issue is seen promptly.

The RMM has the capability to self-remediate certain types of alerts via automation scripts. Alert tickets may be automatically closed by the monitoring application if the alert condition no longer exists. Tickets that are created by Customers or other users never automatically close. Logged tickets are never deleted and maintained for reporting and historical reference within the ticketing system.

Contractual SLAs are defined within the ticketing system based on the agreement defined within the ticketing system. The agreement is based on the signed contract/Work Order with the Customer. The SLA for response time is then automatically tracked by the ticketing system based on status changes for each ticket. SLA status is available on a dashboard within the ticketing system on the Service board screen. Additionally, reports are built into the ticketing system that can be run on demand.

UCS Objective 05: Service Operations Management

05.03: Categorization and Correlation

Problem management policies include procedures for incident/event/alert categorization of tickets to allow for event correlation. Tickets are associated with a Customer when opened, and this association is primarily automated based on either the contact or asset being associated with a specific Customer. The ticket source also indicates the method by which the ticket was opened, whether by call, email, or an automated system. The NOC dispatcher will determine and categorize the ticket by type, sub-type, and item. Tickets may be manually prioritized by dispatch or automatically prioritized by monitoring integrations by setting the prioritization setting on the ticket from Priority 1 as the most important to Priority 5 which is the lowest.

During a notification storm, the correlation of events is handled by an IT Service Engineer and Dispatch. Related tickets may be assigned a parent-child relationship within the Manage platform to consolidate related events into a single ticket while maintaining the history/tracking of each child ticket.

05.04: Support and Problem Resolution

Ticket documentation requirements are defined in the IT Service Operations Manual. Ticket documentation and categorization standards are to be adhered to for all tickets on the Incident, Alert, and INscope service boards. Customer communications concerning tickets are defined in the IT Service Operations Manual.

All updates to Customer tickets made to the Discussion thread of the ticket are automatically sent to the Customer via email. Any updates made by any automated system to the Discussion thread of the ticket is automatically sent to the Customer on the ticket. Ticket close events will also send an email notification to all in-scope tickets informing the Customer that the ticket is closed, and instructions for reopening the ticket if needed.

05.05: Operations Monitoring

A review of tickets for time spent, company assigned, the correct agreement is completed as part of the monthly invoicing process by the VP of IT and the IT Service Manager. Reviews are completed by utilizing Excel exports from the billing system. Managed Service Customers receive either a quarterly or a bi-annual business report. The frequency of the report is determined by the Mainstream Sales Team and the review history is recorded in the PSA. Mainstream utilizes a Custom-built dashboard that pulls data from the PSA to monitor overall operations. These dashboards are real-time web-based reports and are located on the mticw server. These dashboards are available on demand by all engineers and can be displayed on NOC monitors with an automatic refresh as a real-time view into operations. The PSA reports can be/are used by the Director of IT Services and the assigned engineers during informal account reviews for Customers.

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 manage 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	**SuperUser and Administrator Access Security**	✓
06.03	**Revocation of Access**	✓
06.04	**Unique Users and Passwords**	✓
06.05	**Strong Passwords**	✓
06.06	**Segregation of Access**	✓
06.07	**Periodic Review of Access Rights**	✓
06.08	**Secure Remote Access**	✓
06.09	**Network 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

Mainstream's policies and procedures regarding logical access are defined in the sections Data Control and Electronic Access Control, Unique ID and Authentication Methods, and Proper Authentication and Password Management sections of the Mainstream Information Security Policy.

Access provisioning follows Mainstream's set process. The manager of a new employee creates a ticket requesting and approving the employee's access to appropriate applications. The IT Service Engineer creates the initial employee's account and then routes the ticket to other system owners for access to systems that Engineer may not administer.

Requests for changes to user access rights are covered by the Change Control Policy and Procedures within the Mainstream Security Policy. This states that a ticket is created specifying the additional access requested and a justification for the requested access and then approved by the manager of the individual. All requests, approval, and implementation actions are logged within the ticket.

06.02: Super User and Administrator Access Security

Mainstream follows a Role-Based Access Control policy as stated in the Mainstream Security Policy, Administration rights are restricted to accounts only accessible by the Mainstream Technical Services Team to which the administration role has been approved and granted through change control procedures.

Default passwords for any application or device are changed to meet Mainstream's password policy. The passwords are documented in the documentation application or password repository depending upon the role and sensitivity of the password, with the majority of passwords in the documentation application and sensitive passwords in the password repository.

These tools are centrally managed by designated IT management, with access to the passwords being restricted to authorized Mainstream personnel.

06.03: Revocation of Access

Mainstream's termination procedures address the revocation of access rights for terminated and departing employees. A ticket template is used as a checklist for the termination. User accounts are not deleted but marked disabled within Active Directory. Disabled accounts may be removed from Active Directory after one year. Disabling the account automatically disables access to multiple applications using LDAP. All changes regarding the termination process as it relates to revoking access are documented within the Employee Termination ticket.

06.04: Unique Users and Passwords

Shared user IDs and passwords are prohibited as defined in the Information Security Policy. Each employee is required to have their own individual login to Mainstream applications, systems, and services. User Active Directory accounts are created based on a standard naming convention.

Service accounts are described and organized in a particular OU within the domain. The passwords are stored within the documentation application. Access to these accounts is limited by admin rights within the domain. Anonymous, non-unique, or otherwise shared accounts are prohibited by Mainstream.

In compliance-sensitive Customer environments, service personnel utilize a user-unique administrator credential for support and administration functions. For non-compliance-sensitive Customer environments, service personnel are permitted to use a shared administrator credential that is stored in the documentation application or the password repository if the Customer's policy or regulations allows. Access to passwords within the documentation application is tracked as part of that service offering.

06.05: Strong Passwords

Mainstream has a documented password policy within the Information Security Policy. Adherence to password policy is expected practice for all passwords used by all Service/NOC personnel. Password configurations for applications that support inherent authentication are enforced to the extent possible by the applications.

Multiple applications utilize two-factor authentication to reduce Mainstream's reliance on password mechanisms for these applications. The security training application utilizes two-factor for administrative access, but not user access. Internal passwords are enforced via Group Policy in Active Directory.

06.06: Segregation of Access

Access to information systems and the underlying Customer systems and data are separated by functional role to ensure access to resources supports appropriate segregation of duties. This segmentation ensures that development staff does not have access to Customer configuration data and administrative staff only have access to company classification and financial settings within the ticketing system. Access to data is also restricted within the service personnel to those with a business need or in a support role with that Customer.

06.07: Periodic Review of Access Rights

Access to information systems and the underlying Customer systems and data is monitored and reviewed bi-annually to ensure access to resources is restricted to approved personnel, including door security, and in-scope applications. The Physical Security Policy requires that the review be performed at least bi-annually; Mainstream reviews a ticket.

UCS Objective 06: Information Security

06.08: Secure Remote Access

Remote Access to Customer systems is performed using a remote access tool. Access to Customer systems and configuration data is restricted to approved Mainstream personnel via the RMM's login.

Remote Access Sessions are logged by the RMM. Reviews are completed only when an event has been identified by either internal resources or Customers, or when an incident ticket is generated from the SIEM. IP Address filtering is implemented on the RMM to prevent external access to the RMM. The RMM is also protected by two-factor authentication to prevent unauthorized access. If the review is requested by a Customer, the review request and performance would be documented within a ticket. Customers may request a periodic report of access to be generated and sent to them.

06.09: Network Security Management and Monitoring

Mainstream Firewalls are set up with a default-deny policy with rules for business-justified access only. Changes to the firewall configuration must follow Mainstream's security policy and be in a ticket, including business justification, and have approval from XCOM. Routers are configured to allow SSH encrypted connections from Mainstream networks. Internet edge firewalls exist in the Little Rock office and Conway office.

Mainstream network devices and firewall setup procedures are documented within a ticket. The Security configuration requirements are documented in Mainstream's Information Security Policy.

The configuration and technical management of Mainstream network devices and firewalls are performed directly via the respective vendor's proprietary management application. Both the Mainstream network monitoring system and SIEM solution are utilized to monitor the status and security of these devices.

Mainstream provides firewall management and monitoring on a Customer by Customer basis for all managed services Customers. Mainstream also offers firewall-as-a-service for managed services for Customers who choose this option. For Hosting Customers, Mainstream offers both a multi-tenant firewall solution and a dedicated firewall solution.

Mainstream provides an optional multi-tenant firewall service for hosting Customers. The firewall configuration is customized to each Customer's specifications, with changes to the firewall configurations being handled and logged as part of Mainstream's change management procedures. The status of the firewall is monitored via the RMM, which automatically creates alerts tickets based on defined thresholds adjusted as needed by Mainstream. These alerts and notifications are handled as part of Mainstream's defined NOC operational procedures.

SIEM as a service is offered to Security Services customers as well as internally used by Mainstream. Log information is triaged and correlated by an external 24x7 SOC and alerts are routed to a specific Mainstream ticket board (SIEM Board) and recorded in the ticketing system.

06.10: Email Security

Mainstream employs an email security cloud solution to secure internal email and is offered to Customers. The email security solution includes spam filtering, email encryption, attachment scanning, data loss prevention, and business continuity. Alerts generated from the email security solution are typically based on heavy mail flow, with the alerts for the internal email routed to Customer technical contact(s).

Mainstream employs an email security cloud solution to secure internal email and is offered to Customers. The email security solution includes spam filtering, email encryption, attachment scanning, data loss prevention, and business continuity.

Alerts generated from the email security solution are typically based on heavy mail flow, with the alerts for the internal email routed to Customer technical contact(s).

06.11: Antivirus

Antivirus and antimalware solutions are employed to secure assets internally and for all Managed Service Customers. Customers may elect to continue using their antivirus products. The antivirus product is integrated with the RMM and is focused on file scanning for signatures and is always active. This antivirus is complimented by a separate antimalware security solution that serves as a DNS filter that blocks name resolution to known bad URLs/DNS names. The antivirus and antimalware applications are managed via centralized dashboards to provide visibility to all protected endpoints, with alerts from the solutions logged on the Alerts Board and processed following NOC operational procedures.

06.12: Wireless Network Security

Mainstream provides an internal wireless network that is restricted to employees and Mainstream owned devices. Employees must request access to the network through a ticket. Service/NOC personnel will connect the device to the network using a WPA2 pre-shared key.

Guest wireless connectivity is available and requires a pre-shared key that is provided to guests and employees to use on non-Mainstream owned devices. The guest wireless network is a segmented untrusted network that does not have access to Mainstream's internal network and is routed to the internet with a separate firewall and internet provider.

06.13: Network Security Assessments

Mainstream utilizes a partner cloud solution for internal and external vulnerability scans. Mainstream's policy requires that the external scans be performed at least annually and tracked with a ticket. Internal scans are performed weekly, and tickets are automatically created for remediation based on specified criteria. Mainstream also utilizes a SIEM for network security monitoring. This is a near real-time system and triage of tickets is done by the SIEM SOC. Escalated tickets are sent to the ticketing system for remediation.

Internal vulnerability scans are scheduled weekly and remediation tickets are automatically created. Periodic meetings are held to review any remediation issues that require management action to move forward and to review the overall progress of the reduction of vulnerabilities and risk. US-CERT emails for CVE's released for products that are utilized by Mainstream, and Vendor vulnerability announcement emails are also reviewed when received and documented in a ticket.

Network assessments and scans are not part of Mainstream's standard managed services offering but are available as value-added services. Assessments and scans are performed for Customers, based on Customer requests, and are administered with the Customer's application of choice.

As this process is driven based on Customer requests it is documented and communicated via tickets. The responsibility of mitigation and remediation is also customized to the Customer's request. Any remediation work done by Mainstream is logged in a ticket.

UCS Objective 07: Data 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**	x
07.05	**Data Destruction**	*

07.01: Customer Data Backup and Replication

Data backup and replication services provided through GetITBack DR, can be customized per customer request. By default, the off-site backup retentions are set to 7 daily, 4 weekly, and 3 monthly, with 1 off-site backup per day. The standard for local on sight backups with GetITBack DR is to perform continuous incremental local backups every four hours and perform offsite backup and replication daily. The local backup retention policy is set to maintain a minimum of 14 daily versions of backups. In the event of an issue in the GetITBack DR backup and replication process, alerts and corresponding PSA tickets are generated and addressed by Mainstream personnel.

For virtual COLO Customers, the backup policy is defined within the contractual requirements between Mainstream and Customers. The retention policy is to maintain 14 versions of backups locally and take the most recent replica off-site daily. In the event of issues/errors in the virtual COLO backup process, alerts and corresponding PSA tickets are generated and addressed by Mainstream personnel. Customer backups are encrypted both at rest and in transit.

07.02: MSP Data Backup and Replication

All Mainstream internal and Managed Virtualized Infrastructure as a Service Customer's server data backup schedules have been implemented within the backup solution and adhere to Mainstream's standard of maintaining 14 copies of the backup locally and sending an additional copy of the latest version offsite daily. In the event of issues in the internal backup process, alerts and corresponding tickets are generated and addressed by Mainstream personnel. Documentation application backups are taken manually every 2 weeks as a password protected data export and stored on the MTI File server within a protected folder. This task is handled by a scheduled template ticket.

Internal Data Backups are only encrypted at rest if they contain sensitive data. The backups are set up in jobs, and the encryption setting is on the job. The jobs have names to distinguish them from each other. A given machine will only exist in one job; the job definition can be checked and verified that a machine is encrypted. The documentation application is encrypted with a password per the data classification policy by the archive software. All data replications for the backup solution are encrypted in transit by the backup and replication software.

07.03: Data Recovery Testing

Backup data restoration and recovery testing procedures are conducted for internal backups and GetITBack DR Customers on a semi-annual basis. The initiation and results of the testing procedures are scheduled and documented in a ticket.

UCS Objective 07: Data Management

07.04: Disaster and Business Continuity Planning
Mainstream has a documented business continuity plan. Bi-annual file recovery tests are done to verify the ability to recover selected files from the image and documented within a ticket.

Exception Noted: Business Continuity plans must be tested on a periodic basis to ensure the integrity of the MSP. Mainstream Technologies did not test their Business Continuity Plan during the reporting period.

Exception Response: Although Mainstream's Business Continuity Plan (BCP) was not officially tested during the review period, the BCP was exercised in March 2020, when the workforce was notified of a need to transition immediately to a work-from-home posture upon governmental health recommendations regarding COVID-19. Periodic testing of Mainstream's IT Disaster Recovery plan continued throughout the audit period. Formal periodic testing of the BCP has been subsequently scheduled for the Incident Response Team.

Explanation for Requirement Not Applicable:
07.05: Data Destruction
NA- Mainstream does not provide data destruction services.

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 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/Guests**	✓
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

Mainstream has formal policies and procedures governing access to their facility and data center which are documented in the Information Security Policy. Physical security controls are implemented in both Mainstream facilities in Downtown Little Rock and Conway, Arkansas. Controls implemented are as follows:

- Biometric Card Key Access on Exterior doors
- Card Key Access Points to the interior data center doors
- IP Video Cameras.

Access rights of personnel are reviewed and approved by Mainstream on a bi-annual basis which is scheduled and documented within a ticket. If issues are found, they are resolved and documented in the ticket. Mainstream uses the same ticket to generate access reviews of information systems, physical assets, and other items.

08.02: Logging of Visitors/Guests

Visitor and guest logs are maintained at Mainstream's offices through an electronic visitor log system. All visitors and guests are required to register upon entering any building. Visitor logs are available for reporting and review within the visitor log system. All employees and visitors are required to wear a badge while on-site. Upon exiting the facility, visitors are required to log out through the visitor log system. Information gathered includes name, phone, who they are visiting, and whether they are visiting the office or the datacenter. Should the visitor log system be unavailable, a paper sign-in sheet is used.

08.03: Sensitive Area Security

Physical access to the data center is restricted to authorized personnel and monitored via the following mechanisms:

- Doors are locked 24/7, with data center access being restricted to a limited number of personnel within Mainstream.
- Cameras are in place, with cameras recording on motion. Video footage is maintained onsite for review. If a review of the video footage is required, a ticket is created to track and document the review. Monitors showing camera views in real-time are in place.
- The colocation area is physically separated from the rest of the data center. Access to the colocation area is controlled through the badge system and a separate exterior door.

UCS Objective 08: Physical Security

Physical access to any of the Mainstream office space is secured behind biometric door access. Visitors must be let in to gain entry.

08.04: Revocation of Physical Access

Upon termination, employee access to Mainstream's facility is revoked. A member of the Executive Committee will be aware of and communicate any involuntary terminations to the workforce. The Executive Committee coordinates with IT to revoke access while termination is occurring, and actions are tracked within a ticket.

08.05: Data Center Special Requirement: Colocation

Physical access to collocation hardware maintained in Mainstream's facility is restricted to individuals designated by the Customer and authorized Mainstream personnel. The current list of Customer-authorized individuals is maintained within Contacts and the authorized access forms are documented within the Customer's contact folder.

08.06: Data Center Special Requirement: Environmental Controls

Mainstream has implemented the following environmental control systems to protect the data center:

- Smoke/Fire Detectors, with a fire alarm system for monitoring
- Waterless Fire Suppression Systems
- Redundant Climate Control Systems
- Uninterruptible Power Supply Systems
- Backup Generator, Monitored by its own system
- Redundant Power Distribution
- Redundant Data Connectivity/Telecommunication
- Raised Flooring to protect wiring and control temperature

08.07: Data Center Special Requirement: Maintenance

Maintenance contracts are maintained on the backup generator, HVAC systems, Uninterruptible Power Supplies, and FM200 suppression system per supplier recommendations.

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 under 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

All services are provided to Customers within the context of a standard Professional Services Agreement (PSA), which defines billing, confidentiality, and other legal terms and responsibilities of each party, and a collection of associated Work Orders, which describe the specific services, including pricing and service level agreements, to be provided to the Customer. No services are provided to a Customer before the mutual execution of a PSA and Work Order. Changes to the list of services are controlled by the mutual execution of a new Work Order or termination by either party of an existing Work Order. Certain minor changes to the scope of service are allowable as described within the Work Order and are affected by customer-approved requests made in the form of service tickets. Changes to other aspects of a particular service are controlled by the mutual execution of an amendment to the Work Order.

09.02: Accuracy of Service Invoices

Invoices are generated at the end of the month for the just-completed month for all managed services, managed security, and hosting Customers. Invoice amounts are based on the pricing specified in the currently executed version of the applicable Work Order, which defines any fixed-fee amounts, per-unit amounts, and which services are out-of-scope and subject to hourly or additional billing.

09.03: Report Availability

Ticket reports are available to Customers per signed SLAs. Customers have access to tickets and report information through the portal. Mainstream's standard PSA mandates that a periodic relationship review meeting occur at least annually, where reports are provided to each Customer regarding alerts and request tickets resolved during the period. Additionally, Managed Security Customers receive periodic scorecard reports for user awareness training and potential risk from unpatched vulnerabilities.

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 a firm financial footing, as well as risk-averse in a variety of areas unique to managed services and cloud to effectively deliver its services to the Customer.*		✓
10.01	**Operational Sustainability**	✓
10.02	**Significant Customer Risk**	✓
10.03	**Gross Profit Margin of Services**	✓
10.04	**Customer Commitments**	✓
10.05	**Insurance**	✓
10.06	**Customer and Employee Retention Tracking**	✓

10.01: Operational Sustainability

Mainstream was incorporated/formed in 1996 and has been providing managed IT services to Customers for over 16 years. As of the date of this report, Mainstream's 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

Mainstream's top five Customers represent approximately 38% of total Mainstream revenue, which is less than the UCS best practice of 50% from the top five Customers. The largest Mainstream Customer represents only 18% of total Mainstream revenue which is less than the UCS best practice of one Customer not representing more than 20% of total revenue. Due to this, Mainstream is considered to have minimal risk due to the loss of a significant customer.

10.03: Gross Profit Margin on Services

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

10.04: Customer Commitments

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

10.05: Insurance

Mainstream 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, Mainstream has a managed services Customer retention rate of approximately 96% and an employee retention rate of 79%.

SECTION 6: REPORT ADDENDA

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

FOR MAINSTREAM'S SOC 2 MAPPING

This MSP/Cloud Verify Program™ (MSPCV) report for Mainstream Technologies (Mainstream) is based on the control objectives of the Unified Certification Standard for Cloud and Managed Service Providers (MSPs) (UCS) v2020. 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 Mainstream MSPCV report to their SOC 2 report[2]. This table was included in the issued and unqualified 2020 Mainstream SOC 2 Type 2 report on Security, Availability, and Confidentially.

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.	✓	✓	✓							
CC1.5 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										
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.	✓	✓	✓		✓		✓	✓		

[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.

Trust Services for the Security, Availability, and Confidentiality Principles	MSPAlliance UCS Objectives									
	01	02	03	04	05	06	07	08	09	10
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										
CC4.1 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 promptly 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 in 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.						✓		✓		

Trust Services for the Security, Availability, and Confidentiality Principles	MSPAlliance UCS Objectives									
	01	02	03	04	05	06	07	08	09	10
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, considering 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, back-up 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 failed 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.		✓			✓					

Trust Services for the Security, Availability, and Confidentiality Principles	MSPAlliance UCS Objectives									
	01	02	03	04	05	06	07	08	09	10
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										
CC8.1 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										
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	✓	✓		✓						
CC9.2 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.				✓				✓		
A1.2 The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up 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.		✓	✓				✓			
C1.2 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 Mainstream, as described, address the common criteria related to security and the additional criteria related to availability and confidentiality, with the exception of the following:

Trust Services Criteria	Not Applicable Reason
CC 6.0 Common Criteria Related to Logical and Physical Access Controls	
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.	Mainstream does not perform data destruction services; therefore, this requirement is not applicable.

COMPANY INFORMATION

Examined Company:

Mainstream
325 W Capitol Ave Ste 200
Little Rock, AR 72201
Phone: (501) 801-6700
www.mainstream-tech.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®
100 Europa Drive, Suite 569
Chapel Hill, NC 27517
Phone: 800-672-9205
www.mspalliance.com