



MAINSTREAM
TECHNOLOGIES
CREATE • MANAGE • SECURE

Cyber Verify™ Level 3 – Report

Report on Compliance with the MSPAlliance® Unified Certification

Standard for Cloud and Managed Service Providers® v.23

December 1, 2023, to November 30, 2024

Table of Contents

SECTION 1: INTRODUCTION	2
SECTION 2: REPORT BY MANAGEMENT	5
SECTION 3: INDEPENDENT ACCOUNTANT'S REPORT.....	7
SECTION 4: DESCRIPTION OF THE CLOUD AND MANAGED SERVICES ENVIRONMENT.....	10
Mainstream Technologies, Inc. Background	11
Services Offered	11
Services Verified Under Cyber Verify™ Report.....	12
Events Subsequent to the Cyber Verify™ Period of Review.....	12
External Service Providers Not in Scope of Report	12
Explanation of the Cyber Verify™ Certification Table.....	12
SECTION 5: CYBER VERIFY™ CERTIFICATION TABLE	14
UCS Objective 01: Governance	15
UCS Objective 02: Policies and Procedures.....	18
UCS Objective 03: Confidentiality, Privacy, and Service Transparency.....	21
UCS Objective 04: Change Management	23
UCS Objective 05: Service Operations Management	26
UCS Objective 06: Information Security	28
UCS Objective 07: Data and Device Management.....	34
UCS Objective 08: Physical Security	36
UCS Objective 09: Billing and Reporting	39
UCS Objective 10: Corporate Health	40
SECTION 6: REPORT ADDENDUM.....	41
SOC 2 Report Addendum	42
COMPANY INFORMATION	46

SECTION 1: INTRODUCTION



Dear Reader,

The following service provider has successfully completed the MSPAlliance® Cyber Verify™ Program. The Cyber Verify™ Report is based on the Unified Certification Standard (UCS) for Cloud and Managed Service Providers® developed by the MSPAlliance®. For more than 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 Cyber 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 Cyber Verify™ examination must be renewed annually.

There are three levels of examination under the Cyber Verify™ framework: Level 1, Level 2, and Level 3.

Level 1 is self-attestation. This means that the service provider has self-attested to meeting the necessary requirements as of the specified date of its attestation.

Level 2 is a "point in time" examination. This means that the service provider met the necessary requirements as of the specified date of its examination.

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

This Cyber Verify™ 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.



MSPALLIANCE

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 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®

Las Vegas, Nevada

SECTION 2: REPORT BY MANAGEMENT

**REPORT BY MANAGEMENT ON THE SERVICES ENVIRONMENT
FOR THE CYBER VERIFY™ PROGRAM, BASED ON THE MSPALLIANCE® UNIFIED
CERTIFICATION STANDARDS FOR CLOUD AND MANAGED SERVICE PROVIDERS®
LEVEL 3**

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 for the period December 1, 2023, to November 30, 2024. We provide reasonable assurance that Mainstream Technologies, Inc. has met, in respect to the Cyber Verify™ Program, based on the MSPAlliance® Unified Certification Standard for Cloud and Managed Service Providers® v.23 – Level 3, 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 Mainstream Technologies, Inc. Description of the Cloud and Managed Services Environment.

Johnny R. Burgess II, President
Mainstream Technologies, Inc.
Little Rock, Arkansas

SECTION 3: INDEPENDENT ACCOUNTANT'S REPORT

Independent Accountant's Report

To the 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 Cyber Verify Program based on the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers for the period December 1, 2023, to November 30, 2024, is presented in accordance with the MSPAlliance Cyber Verify Program based on the 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 AICPA. Those standards require that we plan and perform 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 was provided by Mainstream Technologies, Inc. management to provide additional information on the corporate health of Mainstream Technologies, Inc.. While objective 10: Corporate Health is part of Mainstream Technologies, Inc.'s description of its cloud and managed services environment and the MSPCV certification table made available to user entities for the period December 1, 2023, to November 30, 2024, the information about Mainstream Technologies, Inc.'s objective 10: 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 Mainstream Technologies, Inc. is provided by Mainstream Technologies, Inc. management to provide additional information and is not a part of Mainstream Technologies, Inc.'s description of its Cloud and Managed Services Environment or the MSPCV Table made available to user entities for the period December 1, 2023, to November 30, 2024. Information about Mainstream Technologies Inc.'s SOC 2 addenda have 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 Cyber Verify Program based on the MSPAlliance Unified Certification Standard for Cloud and Managed Service providers v.23 Level 3, 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 December 1, 2023, to November 30, 2024, Mainstream Technologies, Inc. has met the requirements in respect the MSPAlliance Cyber Verify Program in accordance with the MSPAlliance Unified Certification Standard for Cloud and Managed Service Providers V.23 – Level 3 is fairly stated, in all material respects.

Lovell-Smit & Associates, PLLC

Lovell-Smit and Associates, PLLC
Charlotte, North Carolina
September 19, 2025

SECTION 4: DESCRIPTION OF THE CLOUD AND MANAGED SERVICES ENVIRONMENT

Mainstream Technologies, Inc. Background

Mainstream Technologies provides Full-Service IT Support, Managed Hosting, Infrastructure as a Service, Colocation, Cybersecurity Services, and Software Development services to organizations seeking to optimize, improve and secure their technology assets. Mainstream delivers these services utilizing industry standard methodologies, ensuring a customer friendly and predictable cost model. Mainstream provides these services and solutions to national and regional private sector organizations, and state and local government through four distinct service lines.

Services Offered

Managed Hosting, IaaS, and Colocation Services delivered via a secure data center located in Little Rock, AR.

- Mainstream Technologies Managed Hosting
 - Hardware setup and deployment
 - Server management and administration
 - Patch management and security
 - Data Protection and Backup
 - System and network monitoring

- Mainstream Technologies / Infrastructure-as-a-Service (IaaS)
 - Secure virtual servers
 - Application hosting capability
 - Server management and administration
 - Patch management and security
 - Data protection management, off-site backups and disaster recovery
 - System monitoring

- Mainstream Technologies Colocation:
 - Secured rack or cage within the data center
 - Environmentally controlled, secured, and monitored areas
 - Redundant power and data connections
 - Remote-hands IT support

Information Technology support, consulting, cybersecurity services, data protection and disaster recovery.

- Mainstream Technologies Full-Service IT Support (Managed Workstation & Managed Infrastructure)
 - Server, infrastructure, desktop, and end-user support, via on-site and remote delivery
 - Assessment, planning, implementation, monitoring, and proactive maintenance
 - Hardware and software lifecycle management

- Mainstream Technologies Managed Cybersecurity Services
 - Governance, Risk, and Compliance Consulting (Managed Compliance)
 - Policy Compliance Scanning (infrastructure)
 - Managed Security Information and Event Management (SIEM)
 - Managed Detection and Response (MDR)
 - Managed Endpoint Detection and Response (EDR)

- Managed File Integrity Monitoring
 - Managed Active Directory Integrity Monitoring
 - Vulnerability scanning and remediation
 - End-user Security Awareness Training
- Mainstream Technologies GetITBack Disaster Recovery
 - File and system-level off-site backup services
 - Backup data retention policies
 - System state backups
 - Secure and encrypted transmission of all backup data
 - Mainstream Technologies Software Solutions
 - Custom software design and implementation tailored to meet unique business needs.
 - Expertise in scalable, user-centric solutions aligned with operational goals.
 - Development teams to augment larger programs for on-time, within-scope project delivery.
 - Extensive experience with both cloud native and closely held infrastructures.
 - Seamless system integration for streamlined operations across industries.
 - Mature processes ensuring high-quality, secure, and reliable software.
 - Close client collaboration for clear communication and project alignment.
 - Solutions designed to meet functional, security, and compliance standards.

Services Verified Under Cyber Verify™ Report

This Cyber Verify™ report has been prepared to provide information on Mainstream's compliance with the MSPAlliance® Unified Certification Standard v.23. The scope of this Cyber Verify™ report is on Mainstream's Managed Hosting, Managed Virtual Hosting/laaS, Colocation, Full-Service IT Support, Managed Cybersecurity Services, GetITBack Disaster Recovery, and Software Solutions, in the context of the Cyber Verify™ report, Customers are defined as entities utilizing these services.

Events Subsequent to the Cyber Verify™ Period of Review

Through its membership in the MSPAlliance®, Mainstream completed a Systems and Organization Control (SOC 2) Type 2 Report subsequent to November 30, 2024. 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 relies on the encryption controls and the data storage controls (physical security) of their cloud-based applications. Reference to the services provided by these subservice providers is 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.

Explanation of the Cyber Verify™ Certification Table

In the following Cyber Verify™ 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.23 - Level 3. 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,
- x - Mainstream asserts its compliance with the underlying Requirement is not fully met, or
- * - Mainstream asserts its compliance with the underlying Requirement is not applicable to either the services provided by Mainstream or is not within the scope of the examination.

As part of the Cyber Verify™ process, Mainstream is improving their 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: CYBER VERIFY™ 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, 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 top-level governance and supervision of the company. Board members are selected and affirmed by rank-order voting of outstanding shares. Currently three of the five directors are external, with members of the Executive Committee comprising the balance. The Executive Committee is responsible for strategic development and the day-to-day operations of Mainstream. Executive Committee members are the Vice President of Software Solutions, and the President.

Board meetings are held every 2-4 months (generally quarterly), with agendas published to directors in advance and meeting minutes retained by the President, who serves as the Board Chair. The Executive Committee 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
- Director of Security Services
- Director of Research and Consulting
- Senior Director of Information Technology
- Finance Director

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
- Senior Director of Information Technology
- Director of Information Technology

The Risk Assessment Committee and Information Security Committee both meet on at least a monthly basis. The President retains meeting minutes for both committees.

MSP Leadership meets weekly; The MSP Leadership progress and status are tracked via the EOS VTO document, which is maintained by the President.

The company directory is continuously updated by the Director of Human Resources as part of any onboarding, transfer, and offboarding events. The organizational chart is generated dynamically from the company directory and is always available for viewing on the Associate Portal. All associates are introduced to the Associate Portal during their onboarding.

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 the Executive Committee as well as the personnel within the organization are documented as part of the company directory/organizational chart area of the intranet. The responsibilities are documented to show the management and daily operations duties for which each position is responsible. Executive Committee members, the Senior Director of Information Technology, 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 the MSP to perform their assigned duties.

01.02: Strategic Planning

Strategic plans and priorities are set by the Executive Committee and communicated to the Board via a presentation of the plans and statuses.

Mainstream is implementing the Entrepreneurial Operating System (EOS) to integrate the day-to-day management of the business with long-range Strategic Planning. 3- and 10-year goals for the company and each component business unit and are evaluated and adjusted quarterly, with detailed plans developed to meet upcoming goals. EOS has been fully implemented for the MSP business unit and is being phased in to the ATP unit and administrative functions.

01.03: Risk Management

The Risk Assessment Committee employs a process based on the NIST 800-30 risk assessment framework to assess adversarial and non-adversarial risks, which is integrated with and a process which assesses the Company's maturity relative to its Inherent Risk Profile per the FFIEC Cybersecurity Assessment Tool, in order to identify potential controls and mitigations

and continuously improve the organization's security posture relative to its risk from relevant threats.

The risk assessment process is overseen by the Risk Assessment Committee, which meets regularly throughout the year to complete the assessment work, which culminates with the Annual Risk Assessment report. The Annual Risk Assessment is reviewed by the Executive Committee and then the Board for approval.

01.04: Software Management

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 Microsoft SPLA and VMWare (VSPP).

Licensing is provided under Microsoft Service Provider License Agreement ("SPLA"), VMWare Cloud Service Provider agreement ("VSPP"), and an annual Veeam Service Provider agreement. SPLA and VSPP provider services are reported monthly, and Veeam Service provider services on an on-demand basis. Veeam Service provider agreements renew annually or with physical changes to the host IAAS environment. VSPP licensing are reconciled and reported monthly using documented policies and procedures contained within recurring tickets.

The Director of Information Technology is responsible for completing and reporting the SPLA licensing information based on usage. Calculation spreadsheets are updated as needed. The President is responsible for managing and reviewing the service provider licensing agreements for the MSP.

01.05: External Service Provider Management

Mainstream performs a risk analysis on all potential vendors before signing the contract with the vendor. This is the responsibility of the Risk Assessment Committee. Mainstream sends requests for due diligence to all vendors and stores all due diligence in a designated folder on the shared drive. Once all vendors have submitted their due diligence, Mainstream schedules a meeting internally to review the vendor's due diligence and score the vendors. These vendor scores are documented in the meeting minutes and stored in the same new vendor folder on the shared drive.

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 Mainstream.

Mainstream's 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.

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

Mainstream has documented policies and procedures within their Employment Agreement and Associate Portal. These documents address the following: General terms of employment, including confidentiality, work product ownership, compensation, and leave policies are covered in a standard employment agreement between Mainstream and each associate. Additionally, general policies, information, and HR procedures regarding 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.

HR policies and procedures are maintained on the intranet site, where they are available to employees. The review of these policies and procedures with new hires is tracked with a new hire checklist.

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.

02.02: Incident Response Policies and Procedures

Mainstream's Information Security Policy addresses incident response requirements. Mainstream also 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. This plan includes 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 which 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.

Mainstream stores Customer PII such as contact information, name, email, and phone numbers in the ticketing portal. Certain customer configurations are also stored such as managed firewall and remote access configurations. Access to these managed customer configurations is access controlled using the principle of least privilege. Customer data is stored encrypted with encrypted and audited access in designated technologies outlined in the Software section.

The procedures for response and communication to Customers and other appropriate parties are defined in the Policy and Procedures manual within the Data Breach and Incident Response section. Incidents and communications will be tracked within a ticket.

Mainstream has not made any ransomware payments within 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 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. New policy versions are submitted by the Information Security Committee to the Executive Committee for review and final approval.

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 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: Internal Audit

Mainstream completes an annual internal audit through the Cyber Verify™ Level 3 Audit.

The audit standards verify that the internal controls are being met.

The completed Cyber Verify™ and SOC 2 reports are reviewed and approved by the Executive Committee, which creates action items to address any reported exceptions. The reports and any action items are subsequently reviewed by the Board of Directors.

The Cyber Verify™ report is published on Mainstream's website. Both the Cyber Verify™ and SOC 2 reports are archived in a Company Confidential file share accessible by the Executive Committee, Risk Assessment Committee, and Information Security Committee.

The criteria and scope are documented via the vendor audit portal for Mainstream.

02.05: Employee Acceptance

Each employee must sign their individual 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 on the policy training portal. Associate acknowledgments of receipt and understanding of policy changes are tracked via an internal application.

02.06: Training and Orientation

Mainstream has a formal onboarding program for new hires that is 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 Technologies maintains employee-specific training requirements, updated during regular performance reviews, that define skill level enhancements and areas where additional training may be needed. Continuing education goals are specific to each individual and managed by the Director of Information Technology to ensure the requirement aligns with company goals and customer expectations.

Training may involve internal, self-study, or in-person training by an external service provider. Employees are reimbursed for out-of-pocket training expenses. Additional financial compensation is considered based upon successful completion and/or 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, Data Protection, and Encryption	✓
03.04	Organization Data Geolocation Disclosure	✓
03.05	External Service Provider Geolocation Disclosure	✓
03.06	External Service Provider Management	✓
03.07	External Service Provider Access Disclosure	✓

03.01: Employee Background Check

Pre-hire criminal background, SSN, and OFAC checks are performed for all Mainstream associates. Background checks are also conducted on existing employees by Customer request and are tracked by the Executive Committee 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 Executive Committee 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. All employees must review and acknowledge each new version of the Information Security Policy, which happens at least annually.

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 as part of the new hire process. Furthermore, all new hires are also required to sign an acknowledgement to attest to their understanding and adherence of Mainstream's Information Security Policy and to sign a HIPAA Policy acknowledgment to attest to their understanding and adherence to Business Associate agreements and the associated data. All employees must review and acknowledge each new release of the Information Security Policy, which happens at least annually.

03.03: Data Classification, Data Protection, 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)
- 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 which 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 the remote location. Mainstream stores the encryption passphrases for GetITBack DR Customer backups within the documentation tool. Mobile devices use OS level encryption to encrypt the device drive with the unlock key stored in Active Directory.

03.04: Organization Data Geolocation Disclosure

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

03.05: External Service Provider Geolocation Disclosure

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

03.06: External Service Provider Management

Not Applicable - Mainstream does not allow continuous ESP access.

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.

There were no occurrences of an external service provider utilized by Mainstream having access to a customer system during the review period.

03.07: External Service Provider Access 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.

There were no occurrences of an external service provider utilized by Mainstream having access to a customer system during the review period.

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. 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	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

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. Customer configurations for managed customers are gathered from an RMM tool and synchronized with the PSA system and documentation software.

Customer configuration data is captured during the initial onboarding process as part of the onboarding ticket. Configuration of infrastructure is captured and stored by the RMM. Other configuration data is documented in the document management platform. Configuration data for infrastructure is automatically updated by the RMM when changes are detected.

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

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 identified on the Mainstream website that are referenced in the contracts can be applied with no contract changes or acknowledgement by the Customer. Any necessary contractual changes are processed through either updating the original agreement or the approval of the termination of services noticed. Once the contractual changes have been completed by the Account Management team, a ticket is created to onboard or offboard the services.

04.02: Service Level Categorization

Customers are categorized and identified within the PSA by company type, status, and agreements with corresponding SLAs. Manage agreements are directly configured based on Customer contracts. Modifications to Customer configurations are documented via 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.

04.03: Internal Change Tracking

Mainstream has a formal change management process, documented in the Information Security Policy. Change requests are reviewed and approved by the change control committee consisting of members of the Information Security, MSP, and ATP staff.

The process of submitting a ticket to the ticketing system before its routed to the correct parties for approval.

04.04: Customer Change Tracking

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 PSA.

Customer approval for change requests is based on the customers' requirements

Customers send in a ticket request, and if additional approval is required it is documented in the ticket. If the user that sent in the request is authorized, then the work is assigned to an engineer to perform.

Customers can email in a new ticket for a change, or they can call and ask the dispatcher to open a ticket for the change or they can login to the ticket portal and submit the request.

All changes are documented in and approved if needed using the PSA.

04.05: Capacity Planning

Storage capacity is monitored through the RMM with two-stage alerts that are based on thresholds set within those monitors. When a threshold is reached, a PSA ticket is created by the system and assigned to an engineer. Any storage capacity issue that poses a risk to production availability is worked on according to its pre-defined priority. If the problem can be mitigated via software or data usage changes, those changes are communicated 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 via Mainstream's regular review process and is used as a factor in planning future upgrades and replacements.

04.06: Patch Management

Mainstream utilizes a third-party application to patch all Windows devices for Windows and third-party software. Patches are applied during a regularly scheduled maintenance window, with patch approvals issued before this window. 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, then those requirements are communicated during on-boarding and documented in their PSA 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. Mainstream applies patches one week after their release to allow the community to evaluate patches and to circumvent a vendor recall.

If the patch wasn't recalled in the week following its release and Mainstream does not receive notice of issues, patches are selected and applied during the Customer's maintenance window using an automation tool that logs what patches are applied and when they are applied.

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

Mainstream's IT Service has a defined schedule for customer support staff to cover the published hours of operation. Emergency/after-hours on-call is a set schedule and is rotated between managed services engineers on a weekly basis. This on-call schedule is maintained in an outlook shared calendar.

Mainstream's Network Operations Center and Support Center are staffed by personnel to monitor, log, and respond/resolve issues and incidents. The NOC is located at Mainstream's corporate offices in Little Rock. After-hours alerts are sent via SMS/text to the on-call engineer. After-hours phone calls are handled by a call service and then follow a call tree to reach the appropriate resource. The call service does not have access to Mainstream's systems.

05.02: Support and Problem Logging

Customer support issues are logged 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 business impact on the Customer.

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.

Tickets in the ticketing system must be kept for 5 years. Tickets may be closed, resolved, or canceled. Any engineer can close a ticket upon completion of the work.

NOC alerts are created from monitoring systems and automatically create tickets in PSA. 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 routed 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.

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.

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 automated system. The NOC dispatcher will determine and categorize the ticket by type, sub-type, and item. Tickets may be manually 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 Services Engineer and Dispatch. Related tickets may be assigned to a parent-child relationship within the PSA 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 In-Scope service boards.

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. Mainstream's ticketing system is configured to automatically send ticket updates and closure emails to customers.

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 threads of the ticket are 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. Mainstream's ticketing system is configured to automatically send ticket updates and closure emails to Customers.

05.05: Operations Monitoring

A review of tickets for time spent, company assigned, and correct agreement is completed as part of the monthly invoicing process by the Director of IT. Reviews are completed by utilizing spreadsheet software exports from the billing system.

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 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	Controlled 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	Continuous Review of Access Rights	✓
06.08	Restricted Secure Remote Access	✓
06.09	Network and Endpoint Security Management and Monitoring	✓
06.10	Email Security	✓
06.11	Network and Endpoint Protection	✓
06.12	Wireless Network Security	✓
06.13	Network Security Review	✓

06.01: Controlled Access to Applications and Environments

Mainstream's policies and procedures regarding logical access are defined in the "XIV. - POLICY: ROLE-BASED ACCESS CONTROL FOR DATA, SYSTEMS, AND NETWORK COMPONENTS" sections of the Mainstream Information Security Policy.

Mainstream has the following authentication security mechanisms implemented on its service delivery systems:

- RMM: AD Authentication and MFA
- PSA: AD Authentication and MFA
- Remote Access Tools: AD Authentication and MFA
- SIEM: MFA
- Password Repository: AD Authentication and MFA
- Active Directory: MFA
- CRM: MFA

All applications use Active Directory authentication with MFA if offered, or application authentication (username and password) plus MFA.

Requests for changes to user access rights are covered by the Change Control Policy and Procedures within Mainstream's 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.

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 MSP Service Engineer creates the initial employee's account and then routes tickets to the 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.

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 most passwords in the documentation application and sensitive passwords in the password repository. These tools are centrally managed by designated IT management, with access to passwords being restricted to authorized Mainstream personnel. The password repository tracks anytime a password is accessed and who accessed it. A periodic ticket is generated to review these password access logs for suspicious behavior.

06.03: 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 their own OU within the domain. The passwords are stored within the documentation system. Access to these stored passwords is restricted and logged, with the logs being reviewed quarterly. Service accounts are assigned the minimum necessary permissions to complete the tasks which they were created for.

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 are tracked as part of that service offering.

06.04: 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.

06.05: Strong Passwords

Mainstream has a documented password policy within the Information Security Policy. Mainstream's password policy is as follows: Passwords must be changed every 90 days, History of 4 remembered Passwords, must be at least 12 characters, Passwords must contain three of four categories: English uppercase characters, English lowercase characters, Base 10 digits (0-9), Non-alphabetic characters. The lockout policy is 30 minutes after 6 invalid attempts. Password configurations for applications that support inherent authentication are enforced to the extent possible by the applications. The PSA, RMM, Documentation, and 2FA/MFA applications utilize two-factor authentication to reduce Mainstream's reliance on password mechanisms for these applications.

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 or directory service.

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.

Passwords are allowed to be stored using the company supplied password manager which is set up to enforce MFA, minimum master password length, and iteration counts.

06.06: Segregation of Access

Access to information systems and the underlying Customer systems and data is 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.

Regarding user and logical access to data and tools used in the direct delivery of services to customers, Mainstream defines roles based on access to the products used to deliver specific services:

- The Managed Services Delivery role will define user access to the tools used in the delivery of those services.
- The Managed Security Services Delivery role will define user access to the specific tools used in the delivery of those services
- The Managed Services Administrator role will define admin access to those tools used in the delivery of those services.
- The Managed Security Services Administrator role will administer access to those tools used in the delivery of those services.
- Users who are not assigned one of the above Delivery or Administrator roles will not have access to the tools used in those roles.

06.07: Continuous Review of Access Rights

Mainstream utilizes a recurring PSA ticket that has a set of tasks assigned to Mainstream's application owners, Data Center Engineers, HR, and primary engineer to review admin user listings and access rights for internal applications, data center logical/physical access, and active directory twice per year. The application owners and personnel enter their notes in the ticket.

06.08: Restricted Secure Remote Access

Access to Mainstream Technologies, Inc.'s network is revoked upon termination (voluntary or involuntary) and access is reviewed bi-annually via a recurring ticket.

Mainstream utilizes Control for remote access to Customer environments. Further, Control uses LDAP/AD integration, DUO Dual Factor Authentication, and it is restricted for use by Service Delivery personnel. All Customer remote sessions are logged via Control and stored for 90 days. A remote session report is available upon Customer request and delivered monthly. Remote access to the company's network is only permitted with work-issued equipment and the company's VPN is also secured by DUO Dual Factor Authentication.

06.09: Network and Endpoint Security Management and Monitoring

Mainstream firewalls are set up with a default-deny policy with business rules justified access only. Changes to the firewall configuration must follow Mainstream's Information Security Policy and be in a PSA ticket, include business justification, and have approval from a member of Change Control. Routers are configured to allow SSH-encrypted connections from Mainstream networks.

Mainstream utilizes an MDR for protecting the network with agents installed on all workstations and servers, plus a network appliance that watches north-south traffic at each location egress point. The MDR provides 24x7x365 SOC services to triage alerts and escalates if necessary to Mainstream staff.

Mainstream network devices and firewall setup procedures are documented within a PSA ticket. The Security configuration requirements are documented in the company'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 Customers who choose this option. For Hosting Customers, Mainstream offers both a multi-tenant firewall solution and a dedicated firewall solution.

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 emailed to Mainstream ticket board and recorded in the ticketing system.

06.10: Email Security

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

06.11: Network and Endpoint Protection

Mainstream has implemented an XDR to scan and monitor internal endpoints. The XDR scans and detects for threats, in the event a threat is detected, it will immediately block, quarantine, and attempt the remediation of the threat. If the threat cannot be resolved, a ticket is automatically generated on the Service Desk board for Engineers to investigate.

Full XDR solutions are employed to secure assets for all Managed Service Customers (Customers may elect to continue using their own product). The XDR is managed via a centralized dashboard to provide visibility to all protected endpoints, with alerts integrated directly into the PSA and processed following operational procedures.

06.12: Wireless Network Security

The company has implemented wireless access points that are centrally managed for all office locations utilizing a cloud controller and WPA2 encryption. The SSID and password are stored in a secure note within the company LastPass vault so that only employees can access the information. The SSID is changed anytime an employee separates from the company.

Guest wireless connectivity is available and requires a pre-shared key that is provided to guests and employees to use on non-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 routed to the internet via a separate firewall and internet provider.

06.13: Network Security Review

Vulnerability scans are continuous, and tickets are automatically created when vulnerabilities are found. Mainstream also does an annual penetration test with a third party. The information security policy is under continual review such that it is reviewed in its entirety within a year.

Vulnerability scans are documented within the scanning system with on-demand reports available. Full scans are scheduled, agent-based scans are continuous, and results are automatically pushed to tickets which serve as documented findings. Penetration tests are documented in the report received from the third party, and tickets are created for remediations if required. Policy reviews are documented by the chief security officer.

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 a ticket is created if remediation is needed.

Mainstream utilizes a third party for external penetration testing on an annual basis. Results are reviewed and tickets are created for items that require remediation.

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	Organization 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

Data backup and replication services provided through GetITBack DR, which can be customized per Customer request. By default, the off-site backup retentions are set to 7 daily, 4 weekly, and 3 monthly with one 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.

GetITBack backups are encrypted/immutable. Mainstream Virtualized Infrastructure as a Service Customer's backups have additional immutable backup copies.

The standard for local onsite 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 Manage tickets are generated and addressed by Mainstream personnel.

07.02: Organization 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.

All Mainstream internal server data backups have additional immutable backup copies. 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.

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.

07.04: Disaster and Business Continuity Planning

Mainstream has distinct plans for response and recovery from general Business Continuity incidents (BCP) and for response and recovery from technology disruptions (DRP). The BCP is tested annually via a tabletop exercise as part of our incident response exercises, the results of which are documented and stored. Quarterly tests of the DRP are performed to verify the ability to recover selected files and systems from backup images to the DR infrastructure and are documented within a Manage ticket.

07.05: Internal Data Destruction

The policies for disposal of media are covered in Section XV of the Information Security Policy under the Secure Disposal of Media section.

07.06: Customer Data Destruction

Not Applicable - Mainstream does not provide Customer Data Destruction services.

07.07: Device and Asset Management

Mainstream manages and monitors all internal assets through their RMM. Internal devices are categorized as their own "customer" that is defined as Mainstream. A list of all assets can be exported from this area of the RMM.

Mainstream has a documented Device Policy that defines devices and contains requirements for the management of mobile devices to mitigate the risks associated with mobile devices.

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	Organizational Physical Security	✓
08.02	Logging of Visitors	✓
08.03	Sensitive Area Security	✓
08.04	Revocation of Physical Access	✓
08.05	Data Center Colocation	✓
08.06	Data Center Environmental Controls	✓
08.07	Data Center Maintenance	✓

08.01: Organizational Physical Security

Mainstream's physical security policy is documented in section XXIII. PHYSICAL PROTECTION AND ACCESS CONTROL. Mainstream requires badge plus biometric on exterior doors and badge access on interior doors to secure areas. Visitors must be escorted outside of the entrance area unless they are an approved service provider. All ingress and egress are logged and recorded by access control and video. The list of persons authorized to physically access Mainstream facilities and critical IT resources are reviewed on a quarterly basis to ensure currency and accuracy. The ticketing system is utilized to track changes to the list of all persons with physical access privileges.

Physical security controls are implemented in the Mainstream office in Downtown Little Rock, Arkansas. Controls implemented are as follows:

- Bio-metric Card Key Access on Exterior doors
- Card Key Access Points to the interior data center doors, and
- IP video Cameras.

Recurring template tickets are generated quarterly to prompt system administrators for a review of the physical access list. The access list is reviewed for accuracy and updated as necessary. Review results are recorded in the review ticket.

08.02: Logging of Visitors

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 logout through the visitor log system. Information gathered includes name, phone number, 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. Physical access to any part 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. A ticket is created when the notification is received that someone is leaving, which specifies the last day access is needed by the departing employee. Access is revoked on the last day of employment by badge deactivation and badge retrieval.

08.05: Data Center Colocation

Physical access to colocation 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. 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. The information gathered includes name, phone number, who they are visiting, and whether they are visiting the office or the data center. Should the visitor log system be unavailable, a paper sign-in sheet is used.

08.06: Data Center 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, monitored via SNMP and a scanning application.
- Uninterruptible Power Supply Systems, monitored by a scanning application.
- Backup Generator, monitored by its system software and alerting system.
- Redundant Power Distribution, Redundant Data Connectivity/Telecommunication, monitored by either a scanning application, SNMP monitoring application, or the vendor.
- Raised Flooring to protect wiring and control temperature.

NOC alerts are created from monitoring systems and automatically create tickets in the ticketing system. The interface for the ticket creation is dependent on the monitoring system and includes two-way API and inbound email connector. Non-critical NOC tickets are routed 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 in a timely manner.

08.07: Data Center Maintenance

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

Quarterly Maintenance

- HVAC systems

Semi Annual Maintenance

- Uninterruptible Power Supplies

Annual Maintenance

- FM200 Suppression

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

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 prior to 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 a 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 each month for the 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 in accordance with signed SLAs. Customers have access to ticket 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 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	✓
10.03	Sustainable Profit Margin on Services	✓
10.04	Customer Commitments	✓
10.05	Insurance	✓
10.06	Customer and Employee Retention Tracking	✓

10.01: Operational Sustainability

Mainstream was incorporated in 1996 and has been providing services to Customers for over 28 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 managed services/cloud/SaaS Customers represent approximately 22% of total managed services revenue, which is less than the UCS best practice of 50% from the top five Customers. The largest Mainstream managed services Customer represents only 9% of total revenue which is less than the UCS best practice of one Customer does not represent more than 20% of total revenue. Due to this, Mainstream is considered to have minimal risk due to a loss of a significant Customer.

10.03: Sustainable Profit Margin on Services

Mainstream maintains a positive gross profit margin on its services, which meets the UCS best practice of maintaining a positive gross profit margin. By meeting the best practice, it shows that Mainstream is operationally efficient in its costs of delivering services.

10.04: Customer Commitments

The majority of contracts have a term of 2 to 5 years or more. Mainstream does not utilize month-to-month contracts.

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 Technologies, Inc. has a managed services Customer and Employee retention rate that fits the UCS best practice.

SECTION 6: REPORT ADDENDUM

SOC 2 Report Addendum

MSPAlliance® Unified Certification Standard for Cloud and Managed Service Providers® FOR MAINSTREAM'S SOC 2 MAPPING

This Cyber Verify™ Program report for Mainstream Technologies, Inc. (Mainstream) is based on the control objectives of the Unified Certification Standard for Cloud and Managed Service Providers® (MSPs) (UCS) v.23. 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 Cyber Verify report to their SOC 2 report². This table was included in the issued and unqualified 2024 Mainstream 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										
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	✓	✓	✓	✓	✓		✓	✓		

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.

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.

	✓	✓				✓			
		✓				✓			

COMPANY INFORMATION



Examined Company:

Mainstream

325 W Capitol Avenue

Suite 200

Little Rock, AR, 72201

Phone: (501) 801-3552

<https://www.mainstream-tech.com/>



Independent 3rd Party Auditor:

Lovell-Smit & Associates, PLLC

6201 Fairview Road, Suite 200

Charlotte, NC 28210



Examining Body:

MSPAlliance®

Phone: 800-672-9205

www.mspalliance.com