Department of Veterans Affairs

Medical Care Collections Fund Electronic Data Interchange Transaction Applications Suite (MCCF EDI TAS)

Microsoft Azure Government (MAG) Cloud Infrastructure as a Service (IaaS)
Veterans Health Administration

Critical Decision (CD2) – Service Level Agreement

May 2019

Version 0.6

Revision History

Note: The revision history cycle begins once changes or enhancements are requested after the Service Level Agreement has been baselined.

Date	Version	Description	Author
21-May-19	0.6	Updated project name, cover page details, contract POP, contract number, stakeholders	P. Ganesh
26-Jul-2018	0.5	Final Draft – Ready for Concurrences	T. Fulton
25-Jul-2018	0.4	Updates to Service Description	D. Bennett
23-Jul-2018	0.3	Updates per DRP and ISCP	T. Fulton
17-May-2018	0.2	Updating per review with customer	T. Fulton
16-May-2018	0.1	Initial draft of IaaS Cloud SLA	T. Fulton

Service Level Agreement

Service Name: Medical Care Collections Fund Transaction Applications Suite (MCCF EDI TAS) Period of performance: 01-April-2019 to 31-March-2020 (Option 2) CSP	
Application Code	**MAG (VASI #2137)**
Contact Information	Account for the identification of key Cloud actors including the Cloud Consumer; Cloud Provider; Cloud Carrier, Cloud Auditor and the Cloud Broker. VA Enterprise Cloud Solutions Office (ECSO). ECSO is responsible providing the overall VAEC Azure solution and ensuring terms of this OLA are delivered to VAEC customers and the Veteran. VAEC oversees the contract with the CSP in all aspects of operations to include performance management, maintenance and security. Contract: GS-35F-0884P the task MS Enterprise Agreement (EA). Cloud Service Provider: Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington. It develops, manufactures, licenses, supports and sells computer software, consumer electronics, personal computers, and services. The VA acquires Microsoft products and services, including Cloud Services are through the contract held by Dell (Contract # TAC-17-34590). All Microsoft Cloud Services are provided in accordance with Microsoft's commercial end user license agreement (EULA) which is incorporated by reference in to TAC-17-34590. Microsoft's SLAs are incorporated into its EULA and are available for download here: https://www.microsoft.com/en-us/Licensing/product-licensing/products.aspx ITOPS Department: Enterprise Cloud Service Office and Service Operations – Infrastructure Operations Consumer: Medical Care Collections Fund Transaction Applications Suite Provider: Microsoft EA Contract VA118-17-F-1888 Carrier: Verizon Auditor: Unknown at this time Broker: Dell (Huston Cambron) COR: Randy Brown II (GAL)
Service Level Agreement Duration	This agreement reflects duration based on period approved by the contract stipulations made by the VA Contracting Office in accordance with the specific cloud model.
Requested Service Level (Application)	Routine Support – 99.0% Service Availability

Service Level Agreement Scope	The Service Level Agreement (SLA) delineates a clear and logical linkage of overall service/capability offerings, service targets and goals: • Provides a description of the **Medical Care Collections Fund Transactions Applications Suite (MCCF EDI TAS)** service covered by the SLA for VA Cloud Services. • Defines the service key stakeholders and their roles and responsibilities • Provides period covered by the SLA with the start date of service • Defines the service hours for **Medical Care Collections Fund Transactions Applications Suite (MCCF EDI TAS)** service • Describes key Service Level Targets and Service Level Goals specific to **Medical Care Collections Fund Transactions Applications Suite (MCCF EDI TAS)** that shall be electronically measured and reported to gauge acceptable and degraded service performance • Identifies the key performance indicators (KPIs) for **Medical Care Collections Fund Transactions Applications Suite (MCCF EDI TAS)** service as identified by the service's key business stakeholders • Provides structure for escalations and conflict resolution • Provides guidance on modifications and reviews
Service Description	**Medical Care Collections Fund Transactions Applications Suite (MCCF EDI TAS)** is a cloud-based Service-Oriented Architecture system that delivers Medical Care Collection Fund business services. The platform transitions business logic from existing VistA capabilities to a modernized solution while VistA remains as the authoritative data source. All information under this new platform is only accessible by authorized users on the VA network. Four MCCF EDI lines of business (eBilling, eInsurance, ePayment and ePharmacy) will require financial transaction processing to/from the Financial Services Center in Austin in addition to other web services. The revenue captured by this system provides funding for critical services utilized by veterans at VA Medical Centers. **Additional information:** • Business Level Objectives - Deliver new SOA platform for four MCCF EDI lines of business (eBilling, eInsurance, ePayment and ePharmacy) to perform financial transaction processing. • Service Level Objectives - Confirm that SLA targets established in this SLA can be consistently achieved (as measured by KPIs). • Baseline services - Availability, Response Time, Continuity, Security, Customer Support (including Escalation), Change Management, Reporting as specified in this SLA document • Optional services - N/A for TAS Releases • Customer-unique services - N/A for TAS Releases **Medical Care Collections Fund Transactions Applications Suite (MCCF EDI TAS)** consists of the following sub-services (if applicable): • **None at this time** Hosted by: Microsoft Azure – Cloud Host Tier Support Level: VASI System Criticality – Medium

	Disaster Recovery (DR) Site: No DR listed (These site recovery services are inherited from the MAG FedRAMP Package #: F1603087869.) Disaster Recovery Level: Routine Support ATO and Approval Date: Feb 19th 2019 Service Level Agreement Modification (SLAM): N/A at this time
Identified Stakeholders	**Service Consumer:** Veterans Health Administration (VHA) Organization: OI&T EPMO Financial Services Center Role: Application Owner Operations Chief Name: Jaime Manzano Phone: 512-460-5307 Email: Jamie.Manzano@va.gov Organization: VHA OCC; eBusiness Solutions Role: Deputy Director Development, eBusiness Solutions Name: Frank Annecchini Phone: 816-268-1260 Email: Frank.Annecchini@va.gov **Service Provider:** Office of Information Technology (OI&T) Organization: OI&T Product Development Planning & Analysis Competency Role: IT Project Manager Name: Toby Rudik Phone: 817-706-2992 Email: Toby.Rudik@va.gov Organization: EPMD Health Portfolio Role: Project Manager Name: James Plastow Phone: 801-924-2175 Email: James.Plastow@va.gov **Third Party Contributor:** Microsoft Azure Government Cloud Additional Stakeholders: Financial Service Center (FSC), Enterprise Project Management Office (EPMO), IT Operations and Services (ITOPS), Enterprise Service Desk (ESD), Health Product Support, Infrastructure Operations (IO)

Stakeholder Roles and responsibilities	This SLA element specifies roles and responsibilities of all parties with respect to the SLA, for the service consumer (agency) and cloud providers (at a minimum). Director – System Owner • Overall responsibility for the development, execution, maintenance, activation, and deactivation of the Disaster Recovery Plan (DRP) • Authorizes all changes to the DRP • Determines if manual or secondary processing should be initiated as a temporary method of maintaining business operations • Ensures that an alternate DRP Director is designated Director (Alternate) – MAG Program Manager • Acts on behalf of the DRP Director should the need arise DRP Coordinator – MAG Program Manager • Monitors recovery team activities until the system(s) are recovered at the recovery site • Ensures that recovery operations are being performed consistent with service level agreements / service level requirements • Provides periodic status updates to the DRP Director • Files an after-action report (AAR) upon resumption of normal operations DRP Coordinator (Alternate) – Application Program Manager • Acts on behalf of the DRP Coordinator should the need arise MAG POC – Application Program Manager • Represents the recovery and restoration interests of the affected Service/Business line MAG POC (Alternate) – Program Manager • Represents the recovery and restoration System Administration System Administrators are responsible for related hardware and software installation, configuration, and maintenance in support of automated applications. They evaluate planned changes and systems events to determine impact and corrective action. They also serve as technical authority in systems hardware and software design in support of short and long-range IT activities. • System maintenance • User administration • Monitor system performance (disk usage, central processing unit (CPU), memory) • Creation and/or maintenance of file systems • Backup and restore activities

	Database Administration The Database Administrator is responsible for developing and maintaining an environment in which all applications schema objects reside. The main areas of importance are database instance tuning, security, and contingency planning. Configuration management of all production database objects and the management of the repository in which they reside are also important. The Database Administrator is responsible for: • Database maintenance • Database security • Database instance monitoring and tuning • Production schema monitoring and analysis • Schema object creation in pre-production and production • Develop backup and recovery strategies • Production schema release, configuration, and/or repository management • Develop contingency strategy Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington. It develops, manufactures, licenses, supports and sells computer software, consumer electronics, personal computers, and services. The VA acquires Microsoft products and services, including Cloud Services are through the contract held by Dell (Contract # TAC-17-34590). All Microsoft Cloud Services are provided in accordance with Microsoft's commercial end user license agreement (EULA) which is incorporated by reference in to TAC-17-34590. Microsoft's SLAs are incorporated into its EULA and are available for download here: https://www.microsoft.com/en-us/Licensing/product-licensing/products.aspx
Service Hours	With Cloud services, the customer organization places part of its IT operations/business processes in the hand of outside suppliers in the form of one or more Cloud Service Providers (CSP). Provide detailed understanding for uptime and availability given vendor(s) varied locations and jurisdictions. (Note periods of time, weekends or holidays have different meaning to the providers located in different countries). **Hours of Operation 24x7x365** **Allowable Service Outage Exceptions:** Will allow for planned outages **Allowable Maintenance Windows:** List all planned maintenance windows to include minor and major releases, EO CRISP releases, and any other maintenance: • **To be determined at a later date.** • **Notification:** Extended release windows can be requested by OI&T with no less than 30 days advanced notice, approved by the Customer no later than 7 days after request **Additional Maintenance Windows (Interdependent Systems):** • **None at this time.**

<table>
<tr><td>Cloud Platform Criteria</td><td colspan="3">SPECIFIC CLOUD COMPUTING PERFORMANCE TARGETS ARE ADDRESSED IN THE PROVIDED ADDENDUM.</td></tr>
<tr><td>Level of Service and Service Level Targets and Goals</td><td colspan="3">Level of service (e.g., service availability):

In accordance with the Online Services Terms (OST), incorporated into the Enterprise Agreement by reference, VA will have the ability to access and extract Data stored in each Online Service at all times during the term of VA's subscription. Upon the expiration or termination of your subscription, Microsoft will preserve VA's data in a limited function account for 90 days so that you may retrieve your data.

The OST also details privacy and security measures Microsoft has implemented and will maintain and follow for all of its Online Services, including policies around organization of Information Security, Asset management, Human Resources Security, Physical and Environmental Security, Access Control, Information Security Incident Management and Business Continuity Management.

• Availability. Percentage of uptime for a service in a given observation period. Availability is typically a heartbeat test: checking to see if the service and its components are alive. Testing can take the form of pings, port checks, launching URLs, or any other test that establishes the service is available.

Level of Cloud Capacity and capability: To be determined (TBD) at a later date

Response Time

Elapsed time from when a service is invoked to when it is completed (typically measured in milliseconds). Measuring response time performance goes beyond simply testing for availability and is best accomplished by interacting with an application, for example, by using synthetic web transactions. It is important to verify both that the expected content is returned and that the response time is within acceptable limits in order to verify that the service is functioning and responsive.

List the Service level Target (SLT) as provided by the business and agreed to by OI&T and Service Provider. List the Service Level Goals (SLG) as defined by the key business stakeholders. All SLTs and SLGs presented below will be reported on a dashboard.

A target and goal will also be set for degraded service/performance. The system will be considered degraded when greater than 0% or less than 5% of users are affected. The system will be considered down when 5% or more of users are affected.</td></tr>
<tr><td></td><td>Target Area 1: Service Availability (application)</td><td>>=99.0%</td><td>>=99.0%</td></tr>
<tr><td></td><td colspan="3">Additional service level targets may be added as needed.</td></tr>
</table>

Key Performance Indicators (KPI)	A KPI is used to determine how you are performing against your business objectives. Any metric which has the ability to directly impact an important outcome (e.g. customer service) can be a KPI. KPIs are optional and only the business can determine them. For example, for VBMS, a KPI could be the average time for application for benefits to be processed. List the metrics that are used to measure the achievement of the Critical Success Factor (see CSF in definition of terms) as defined by the business. All KPIs presented below will be reported on a dashboard.	
	KPI 1: TBD	**TBD**
	Additional key performance indicators may be added as needed.	
Service Continuity; Outages and Disaster Recovery	This SLA element describes how service/capability continuity and outages will be managed by the provider with regard to disaster recovery (DR) and continuity of operations (and address risk management). DR must offer disaster recovery capabilities for the services (IaaS, PaaS) offered. The DR capabilities must include all required hardware and software at the DR site, and suitable data replication mechanisms and processes required to instantiate the configuration at the DR location consistent with the Recovery Time and Recovery Point Objectives (RTO and RPO) defined by the VA DR standards for High, Medium, and Basic tiers. Include agency disaster planning actions accounting for: **How is service outage defined noting what constitutes an outage:** An unplanned event that causes an information system to be inoperable for an unacceptable length of time. **How is customer compensated for an outage:** System owners and users are notified of an outage and a thorough outage assessment is performed for the system. Information from the outage assessment is presented to system owners and may be used to modify recovery procedures specific to the cause of the outage. **What level of redundancy is in place to minimize outages:** Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage, potential for further disruption or system damage, and an expected recovery time of MAG. The outage assessment team conducts this outage assessment. Assessment results are provided to the ISCP and DRP coordinator to assist in the coordination of the recovery of MAG. **What constitutes a disaster:** Disasters are referred to as an emergency that jeopardized IS Services and Operations. **Address and incorporate Disaster Recovery Plan:** The MAG DRP may be activated if one or more of these criteria are met: • The SaaS provider requires a system recovery via offsite back up; • Any or all critical IS Services will not be available within the accepted RTO	

	set forth in the individual ISCPs. Additionally, the decision to activate the MAG DRP may require the DRP director to consult with the service/business Line POC's . **Identify how often provider testing of disaster recovery and business continuity plans take place:** All DRPs should be reviewed and tested at least yearly or whenever there is a significant change to the system. Full functional tests of systems are normally failover tests to the alternate locations and may be very disruptive to system operations if not planned well. Other systems located in the same physical location may be affected by, or included in, the full functional test. It is highly recommended that several functional tests be conducted and evaluated prior to conducting a full functional (failover) test. A formal test plan is developed prior to the tabletop or functional test and exercise. Functional test procedures are developed to include key sections of the DRP and MAG ISCP, including a walk-through of the following: • Notification procedures • System recovery in an alternate MAG region • Internal and external connectivity • Reconstitution procedures Account for additional Precautions (as feasible): 1. **Replicated data stores:** It is important that all backup and installation media used during recovery be returned to the offsite data storage location (as applicable). The offsite data storage procedures should be followed to return backup and installation media. As soon as reasonable following recovery, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup will become the source record and will be stored with other system backups. 2. **Multiple redundant networks:** Recovery sites and offsite storage are required for High and Moderate systems, optional for low systems, and have been established for this system. 3. **Multiple app instances:** TBD 4. **Automated failover:** TBD Include: **Recovery Point Objective(RPO): 24 hours** **Recovery Time Objective (RTO): 30 days** **Maximum Tolerable Downtime (MTD): 30 days** per event
Security and Risk Management	Link to information security policy: <MS Azure OLA>. This SLA element specifies information relating to the confidentiality and integrity of the services and the security controls which apply to the services. VAEC as the Service Provider lists performance indicators monitored internally for this service in Section 5.5. Reporting on

	these metrics will take place (daily, monthly, quarterly, or an agreed upon interval) and made accessible based on the agreed upon terms and conditions. Audits may be performed to examine the execution of service level agreements to determine the extent that they are: achieving business requirements in accordance with contractual terms, conditions and deliverables; are compliant with VA standards for service delivery and security; and are measured for performance and the resulting metrics reported to executive management on a regular basis. Microsoft conducts audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data. Upon request, Microsoft will provide Customer with each Microsoft Audit Report so that Customer can verify Microsoft's compliance with the security obligations under the contract. Microsoft also follows the third party assessment (3PAO) process under FedRAMP. The 3PAO and the FedRAMP continued monitoring requirements amount to a level of control that no other program provides and that can be easily equated to an audit. FedRAMP and the 3PAO processes were designed so that individual agencies would not need to conduct separate audits. FedRAMP is precisely meant to provide a detailed level of scrutiny in the systems. As a result, Microsoft does not allow customers to audit our facilities but do provide detailed audit collateral, including results of monthly scans of Microsoft systems which provide detailed information about software and hardware deployed within the environment covered by the ATO. See the Microsoft Audits of Online Services Section in the OST. In addition, detailed audit collateral is available directly to VA, including ISO, SOC, FedRAMP, ISMS, Whitepapers and FAQs. See https://microsoft.com/en-us/TrustCenter/STP/default.asp. Microsoft does not allow customers to audit its datacenters. If VA believes Microsoft has failed to meet its SLA(s), then the VA must notify Microsoft within the stated warranty period. See the warranty section of the Microsoft Enterprise Agreement and the applicable SLA(s) incorporated by reference into that agreement. Security Requirements Notification The terms governing security notifications for Microsoft cloud properties are incorporated by reference from the Microsoft Enterprise Agreement as described in section 1.3 above. Specifically, the Online Services Terms, which are incorporated into the Microsoft Enterprise Agreement, contains sections on Microsoft's Information Security Incident Management policies and processes. Security Incident handling is also covered under FedRAMP and documented in Microsoft's FedRAMP package(s). See

	control IR-06, wherein Microsoft will support the reporting guidelines in the US CERT - Federal Incident Reporting Guidelines for reporting times (http://www.us-cert.gov/government-users/reporting-requirements.html). Further details are included in the FedRAMP System Security Plans (SSPs). Non-compliance The terms governing SLA Claims for downtime for Microsoft cloud properties are incorporated by reference from the Microsoft Enterprise Agreement as described in section 1.3 above. See specifically, the Claims and Services Credits section. Each discrete service has distinct terms as outlined in the Service Level Agreements for Microsoft Online Services. https://www.microsoft.com/en-us/licensing/product-licensing/products.aspx NOTE: The security of the services NOTE: The security of the services offered must meet or exceed VA standards for systems and services rated at FISMA High level capable of storing sensitive data, as well as data containing PII and PHI information.
Customer Support	Technical help desk support for **Medical Care Collections Fund Transactions Applications Suite (MCCF EDI TAS)** service is required **24** hours a day, **7** days a week, and **365** days a year. VA will utilize its existing Tier 1 Help Desk infrastructure to receive and track initial requests and incidents.
Escalation	**Immediate Escalation:** Once the Enterprise Service Desk (ESD) is made aware of an Incident, it will follow established Procedures to ensure proper resolution or escalation within established timeframes. **Unresolved Escalation Issues:** For any additional issues not reaching resolution, the AAR will be forwarded to the VA governance group for resolution (Reference section pertaining to Conflict Resolution in SLA)
Change Management	Any party to this agreement may request changes at any time by submitting a request in writing to the VA governance organization. The technical description of availability (what components are monitored, measured, and reported) does not require a formal SLA change. Requests to change/add to what is monitored must be sent to the VA governance agency who will schedule a meeting with OI&T and the VA Contracting Office. **The goal is to reach a mutually agreeable solution based on date to be determined by the Contracting Office.**
Conflict Resolution	Either the customer or the service provider may request a meeting with the VA governance agency to address and resolve any conflicts that may arise that is not able to be resolved via normal processes and channels. A formal request shall be made to the VA governance agency Secretariat, and shall include a detailed explanation or the issue(s) along with documentation to

	point out the conflict. The VA governance agency will schedule a meeting with all pertinent parties and the VA governance agency shall act as mediator for the event. Final determination and resolution shall be made by the VA governance agency.
Reporting	Monthly reporting shall be provided aggregating the previous month's results and providing an average of performance results that can be weighed against the maximum and desired response times and availability. Root Cause Analysis Problem Reports are required within twenty four (24) hours of a serious outage, describing the root cause of a particular incident or sequence of incidents. A serious outage is defined as a Critical Event per the National Service Desk (NSD) ticketing system. An After Action Report shall be provided by the NSD and distributed through normal distribution channels. An annual meeting shall be scheduled by the VA governance agency and shall include identified members of both the customer and service organizations responsible for **Medical Care Collections Fund Transactions Applications Suite (MCCF EDI TAS)**. The representatives agree to attend the review meetings, or they agree to send a suitable and prepared alternate representative. The purpose of the meeting shall be to have an open dialogue between customer and provider to discuss overall performance of the service and particular concerns over trends and/or issues. Attendees shall be prepared with questions and responses based on the information documented in the reports. The ultimate goal of the meeting shall be to gain an understanding of customer pain points that lead to improvements in service design and management to align the needs of the business to the capabilities of IT services.

Definition of Terms

Agreed Service Time – The total agreed time that a service will be readily available for use. For example, typical service times may include: 24/7/365 (525,600 minutes of availability per year) or normal business hours, typically 8 hours daily (125,280 minutes of availability per year). Agreed Service Time can be customized based on time zones, recognized holidays, business need, etc.

Availability – The ability of the Cloud service or other configuration item to perform its agreed-upon function when required. This means that users are able to complete tasks as advertised and/or within the reasonable amount of time expected.

- Availability will be calculated as Agreed Service Time minus Unplanned Downtime divided by Agreed Service Time times 100 (to express it as a percentage)
- Agreed Service Time is Total Time less Planned Downtime (see definitions below)
- The Cloud Provider must provide planned maintenance times for subject service and dependent systems for exclusion from the availability and degraded service calculations
- The technical description of availability (what components are measured/monitored) is maintained by the VA governance agency. The Enterprise Program Management Office (EPMO) is responsible for measuring/monitoring on the technical description of availability and following prescribed formulas for calculating availability.

Cloud Infrastructure as a Service (IaaS): The capability available to the consumer is to provide processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Cloud Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Degraded Service – Condition that exists when one or more of the required service performance parameters fall outside of predetermined limits resulting in a lower quality of service.

Degraded Service Time:

- Includes time when features of the service are unavailable, but the entire service is not unavailable
- Includes response times greater than three standard deviations from the average response time
- Includes time when the service is unavailable
- The system will be considered degraded when greater than 0% or less than 5% of users are affected.

Downtime – A period of time during which the users of a business system cannot use the system to perform their work. Downtime can be either planned or unplanned.

- **Planned Downtime** Includes Planned Maintenance Time for normal service on a respective system; Includes Planned Maintenance Time for scheduled maintenance on upstream systems to which the service is dependent
- **Unplanned Downtime** Includes all unplanned outages, including upstream outages; Includes a significant number of errors reported over a set duration of time; Includes the excess time from scheduled release / maintenance windows that extend beyond allotted time, including the service and its upstream systems; Includes system-wide or near system-wide events, and can be national or regional in scope
- The system will be considered down when 5% or more of users are affected.

IT Business Service – Provided to one or more business units by IT. It is based on the use of Information Technology and is made up of a combination of IT Technical Services (applications, infrastructure and resources) that collectively support a function of the business.

Key Performance Indicators (KPI) – A KPI is used to determine how you are performing against your business objectives. Any metric which has the ability to directly impact an important outcome (e.g. customer service) can be a KPI. KPIs are optional and only the business can determine them. For example, for VBMS, a KPI could be the average time for an application for benefits to be processed.

Maximum Tolerable Downtime (MTD) – The total amount of time that a business process can be disrupted without causing any unacceptable consequences. Note: See Diagram of Disaster Recovery terms below.

Recovery Point Objective (RPO) – The maximum tolerable period in which data might be lost from an IT service due to a major incident. Acceptable data loss between backups - Example: With an RPO of 2 hours and If there is a complete replication at 10:00am and the system dies at 11:59am without a new replication, the loss of the data written between 10:00am and 11:59am will not be recovered from the replica. This amount of time data has been lost has been deemed acceptable because of the 2 hour RPO. This is the case even if it takes an additional 3 hours to get the site back into production. The production will continue from the point in time of 10:00am. All data in between will have to be manually recovered through other means. Note: See Diagram of Disaster Recovery terms below.

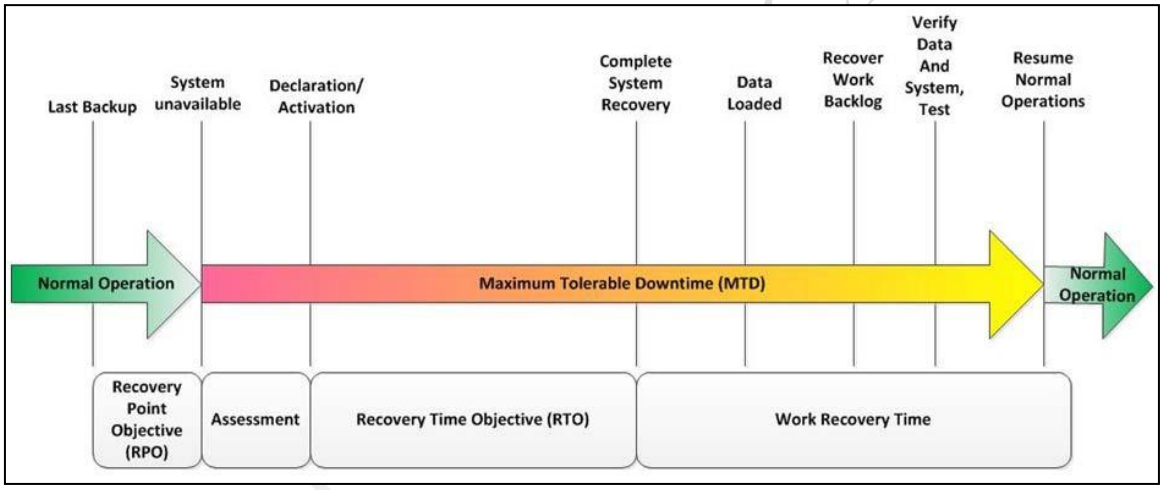
Recovery Time Objective (RTO) – The duration of time and a service level within which a business process must be restored to at least the RPO after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. Note: See Diagram of Disaster Recovery terms below.

Service Level Requirement (SLR) – A customer requirement for a measurable aspect of an IT Service such as performance, capacity, or availability. Service level requirements are based on business objectives and used to negotiate agreed service level targets. Even if provider cannot meet the SLR, the SLR remains intact as evidence of what customer requires and requested.

Service Level Target (SLT) – Service level targets are based on service level requirements, and are the measureable service objectives that can be met given the available infrastructure.

Service Name – Title for the service being provided.

Diagram: Disaster Recovery Terms



Medical Care Collections Fund Transactions Applications Suite (MCCF EDI TAS)

SLA REVIEW AND CONCURRENCE:

The parties below reviewed the **Medical Care Collections Fund Transactions Applications Suite (MCCF EDI TAS)** SLA and concur.

Dwight O. Maloy 215859

Digitally signed by Dwight O. Maloy 215859
Date: 2019.05.23 07:47:03 -05'00'

Digital Signature Required

Jamie Manzano — Date

Chief, EPMD FSC Operations and Maintenance Division

James S. Plastow 398558

Digitally signed by James S. Plastow 398558
Date: 2019.05.23 07:49:59 -06'00'

Digital Signature Required

James S Plastow — Date

IT Project Manager, OI&T EPMO

Digital Signature Required

Jarvis Newsome — Date

Service Level Manager, OI&T Customer Relationship Management

Office of Information and Technology