Phase 2 Comprehensive Maintenance and Operations Plan (CMOP)

Buffalo, NY ITS4US Deployment Project

www.its.dot.gov/its4us.htm

Final Report – November 12, 2024

FHWA-JPO-23-107

ITS4US

IT'S TRANSPORTATION FOR ALL OF US

U.S. Department of Transportation

Produced by NFTA
U.S. Department of Transportation
Intelligent Transportation Systems Joint Program Office
Federal Highway Administration
Office of the Assistant Secretary for Research and Technology
Federal Transit Administration

Notice

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-23-107	(Delete and insert information here or leave blank)	(Delete and insert information here or leave blank)

4. Title and Subtitle	5. Report Date
Phase 2 Comprehensive Maintenance and Operations Plan (CMOP) Buffalo, NY ITS4US Deployment Project	November 12, 2024
	6. Performing Organization Code (Delete and insert information here or leave blank)

7. Author(s)	8. Performing Organization Report No.
Polly Okunieff (ICF), Lina Abounassif (ICF), Nayel Urena Serulle (ICF), Darlene Magold (Etch), Adel Sadek (UB), Kyeongsu Kim (RSG), Robert Jones (NFTA), Kelly Dixon (GBNRTC), Jamie Hamann-Burney (BNMC)	(Delete and insert information here or leave blank)

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
NFTA, 181 Ellicott Street, Buffalo, NY 14203 BNMC, 640 Ellicott Street, Buffalo, NY 14203 ICF International, 9300 Lee Highway, Fairfax, VA 22031 ETCH, 4696 Smothers Road, Westerville, OH 43081	(Delete and insert information here or leave blank)
	11. Contract or Grant No. 693JJ32250011

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
U.S. Department of Transportation ITS Joint Program Office 1200 New Jersey Avenue, SE Washington, DC 20590	Final Report
	14. Sponsoring Agency Code HOIT-1

15. Supplementary Notes

Elina Zlotchenko (USDOT ITS-JPO) is the Award Officer Representative (AOR) and Sarah Tarpgaard (USDOT) is the Award Officer (AO)

16. Abstract

The Buffalo NY ITS4US Deployment Project seeks to improve mobility to, from and within the Buffalo Niagara Medical Campus by deploying new and advanced technologies with a focus on addressing existing mobility and accessibility challenges. The technologies to be deployed are self-driving shuttles, a trip planning app that is customized for accessible travel, intersections that use tactile and mobile technologies to enable travelers with disabilities to navigate intersections, outdoor and indoor paths and destinations. The deployment geography includes the 120-acre Medical Campus and surrounding neighborhoods with a focus on three nearby neighborhoods (Allentown, Fruit Belt and Masten Park) with underserved populations (low income, vision impaired, deaf or hard of hearing, wheeled mobility device users and older adults).

The purpose of the Comprehensive Maintenance and Operations Plan (CMOP) is to describe the operations and maintenance of the configurable items and systems deployed in the Buffalo, NY ITS4US Deployment project -- the Buffalo All Access System. The CMOP provides a high-level overview of the operations and maintenance policies, procedures, roles/responsibilities, and risks associated with each system and component. The CMOP also includes an Issues Management Process (IMP) to manage and delegate issues, anomalies and defects to the appropriate subsystem or component operators and maintainers.

17. Keywords	18. Distribution Statement
ITS4US; deployment; ITS; Intelligent Transportation Systems; Operations; Maintenance; Operations and Maintenance Plan	(Delete and insert information here or leave blank)

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	98	N/A

Revision History

Name	Date	Version	Summary of Changes	Approver
Buffalo, NY ITS4US	5/31/2024	0.1	Initial Draft (working)	Kelly Dixon
Buffalo, NY ITS4US	10/29/2024	0.2	Final Draft – Update CoB MOU and SDS sections. Respond to USDOT Comments	Kelly Dixon
Buffalo, NY ITS4US	11/12/2024	1.0	Final – Edited for additional clarity	Kelly Dixon

Table of Contents

List of Tables

List of Figures

1. Introduction

The purpose of the Comprehensive Maintenance and Operations Plan (CMOP) is to describe the operations and maintenance of the configurable items and systems deployed in the ITS4US Buffalo All Access System. The CMOP provides an overview of the operations and maintenance policies, procedures, roles/responsibilities, and risks associated with each system and component. The CMOP also includes an Issues Management Process (IMP) to manage and delegate issues, anomalies and defects to the appropriate subsystem or component operators and maintainers. The IMP is described in **Section 3.**

Major parts of the Buffalo All Access system are integrated into existing services provided by the project's infrastructure, owner and operator (IOO) stakeholders, or services contracted by external vendors. Roles and responsibilities and service level agreements associated with external or contracted systems are included in **Section 8** for contracted services and **Section 7** for Memorandum of Understanding (MOU) agreements with public and IOO partners.

The two major systems covered in more detail by the CMOP include the cloud deployed open source software Buffalo All Access App (aka Complete Trip Platform (CTP)) (**Section 4**) and Performance Measurement Dashboard (PMD) (**Section 5**).

2. System Overview

The Buffalo All Access System is composed of four subsystems: Smart Infrastructure, CTP, Community Shuttle, and PMD—see **Figure 1** for a high-level context diagram. The subsystems and their components are described in **Table 1**.

Table 1. All Access System Components.

Subsystem	Description
Buffalo All Access App (CTP)	**Trip planning and journey tool** includes website/mobile app with tailored pre-trip planning, reservations, trip execution, and reporting services
Community Shuttle	**Niagara Frontier Transportation Authority (NFTA) On-Demand Community Shuttle** (or Human Driven Shuttle (HDS)) which provides on-demand and door-to-door service **Self-Driving Shuttle** (SDS) which provides flex / microtransit service
Smart Infrastructure	**Transportation Information Hub** (TIH) or kiosk at NFTA's Summer-Best station and Buffalo General Medical Center (BGMC) **Pedestrian Crossing** (PED-X) at 2 intersections – Best/Main streets and Ellicott/High streets **Indoor Navigation System** (INS) technologies in public spaces at Visual Impairment Association (VIA) and BGMC
Performance Measurement Dashboard	Public portal and dashboard available through link from the All Access web page (Uniform Resource Locators (URL)) Private data storage with restricted access

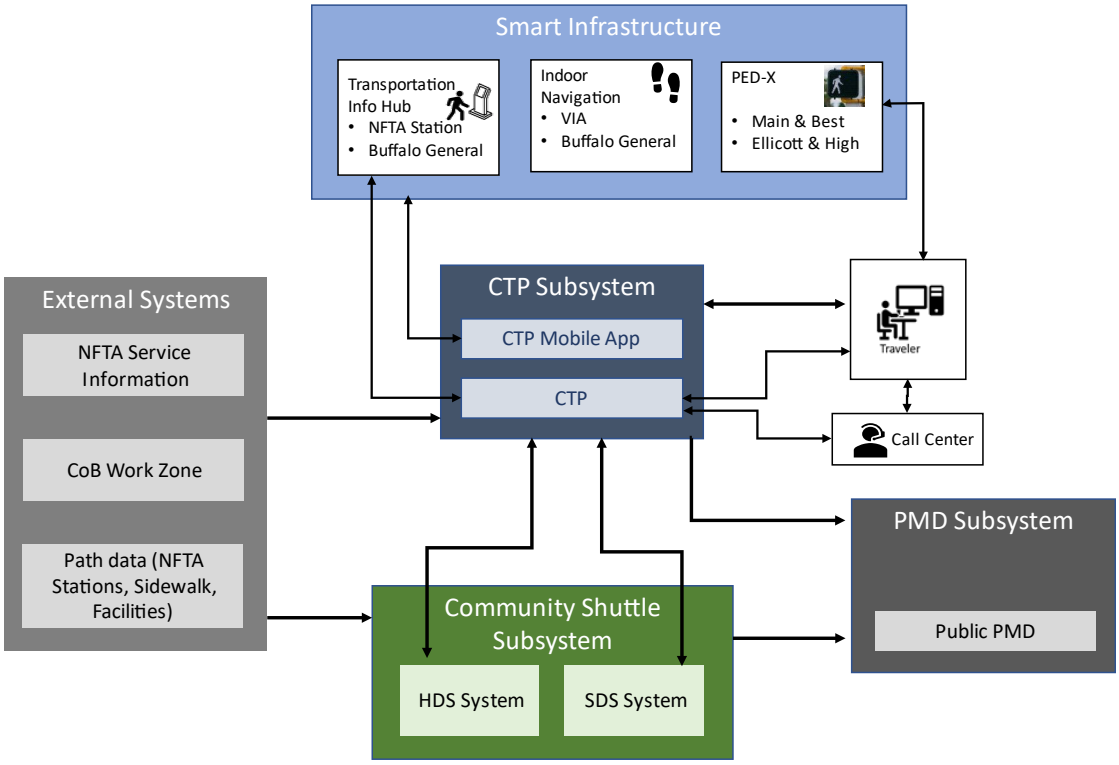


Figure 1. Buffalo Deployment Project Context Diagram
Source: Buffalo, New York (NY) ITS4US

The following documents provide additional information about each subsystem

System Architecture Document (SAD) – physical and functional architecture diagrams, descriptions, information flows and communications protocols. Note: these are not implementation architectures.

System Design Document (SDD) – design for each software subsystem developed through the project, and description of off-the-shelf, software as a service or turnkey components / subsystems.

Interface Control Document (ICD) – description of each interface and its origin-destination.

Comprehensive Installation Plan (CIP) – description of configuration and installation procedures for the INS beacons, Miovision cameras (PED-X), and RedyRef kiosk (TIH).

This CMOP covers the CTP and PMD Subsystems. All other Systems (e.g., Smart Infrastructure, call center, Community Shuttle and External Systems) are contracted operations and maintenance services. **Section 2.1** describes the nature of the contracted services while **Section 2.2** specifies the responsibilities that are covered by contracts or leveraged services from other organizations.

2.1. Systems Not Covered in CMOP

Services that are contracted through service contracts or MOUs are not covered by the CMOP. **Table 2** list these services and provides the information for each:

- Component (or subsystem) – the component (device) or subsystem not covered by the CMOP.
- Responsible Party – the organization who is responsible for the operations or maintenance. In some cases, the operations and maintenance are delegated to different responsible parties.
- Agreement Type – the type of agreement.
- Hardware Maintenance – the type of hardware maintenance (e.g., routine – cleaning, preventive, corrective, replacement).
- Software Maintenance – updates for specific software products and system configurations (software).
- Operations – the type of operations including staff assignments, system and security monitoring and training.

Table 2. Maintenance and Operations Not Covered by CMOP

Component	Responsible Party	Agreement Type	Hardware Maintenance	Software Maintenance	Operations
Self-Driving Shuttle	ADASTEC Corp.	Turn-key contract	ADASTEC – complete hardware maintenance including preventive and corrective activities.	ADASTEC – complete software maintenance activities including preventive and corrective.	ADASTEC – see Section 8.1
TIH	RedyRef	Gold Level Support	Replacement	Updates for Engage (kiosk) software	Monitoring (operations, cyber security)
TIH	Facility Owner (NFTA/BGMC)	MOU	Routine (e.g., cleaning, manage vandalism to power/communications)	n/a	Physical security monitoring, communications and power
Indoor Navigation	CXApp	Annual	n/a	Updates for Software Development Kit	Cloud services (including cybersecurity and monitoring)
Indoor Navigation	Facility owner (BGMC or VIA)	MOU	Replacement (spare beacons provided by project)	Updates to facility layout and paths	n/a

Component	Responsible Party	Agreement Type	Hardware Maintenance	Software Maintenance	Operations
NFTA On-Demand Shuttle	NFTA	Existing services / MOU	Preventive, corrective and replacement maintenance of vehicles and internal components	n/a	Operations, operator staffing, training
Miovision / PED-X gateway	City of Buffalo	Existing services / MOU	Preventive maintenance for Miovision Core Detection and Counts Module and camera	Updates for Server	Monitoring, signal systems
Call Center	VIA	Contracted services / MOU	n/a	n/a	Training, staffing
Private PMD	University at Buffalo (UB) Information Systems (UBIT)	Existing Services	n/a	n/a	Security (access / authentication / monitoring) Backup and recovery

2.2. Contracted Operations and Maintenance Roles and Responsibilities

The contract or agreements governing operations and maintenance roles and responsibilities for system components are listed in **Table 3**. The table includes the following fields:

- **System** – subsystem or components
- **Role** – operations or maintenance
- **Organization** – responsible agent
- **Responsibilities** – list of activities for which the organization is responsible for
- **Governed by** – the agreement or contract governing services.

Table 3. Contracted Operations and Maintenance Roles and Responsibilities

System	Role	Organization	Responsibilities	Governed by
Automated Community Shuttle	Operations	ADASTEC	Turn-key system – data, software, vehicle and operator operations	Contract (Section 8.1)
Automated Community Shuttle	Maintenance	ADASTEC	Turn-key system – vehicle and software	Contract (Section 8.1)

System	Role	Organization	Responsibilities	Governed by
On-demand Shuttle	Operations	NFTA	Leveraging NFTA resources for operations including • Vehicle operations • Driver operations and Standard Operating Procedures (SOP) • Incident Recovery and SOP • NFTA Service Center	NFTA
On-demand Shuttle	Maintenance	NFTA	Leveraging NFTA resources for vehicle maintenance and operator's mobile data terminals	NFTA
INS	Operations	CXApp	Operate Software as a Service (SaaS) for Indoor Navigation and asset inventory	Contract (Section 8.2)
INS	Maintenance	CXApp	Update Software Development Kits (SDK) if change to mobile platforms	Contract (Section 8.2)
INS	Maintenance and Operations	Facility Owner	• Update map based on changes to facility map • Maintenance and security of beacons • Operations of power and WiFi (internet access)	MOU (Sections 7.2 and 7.3)
TIH	Operations	RedyRef	Commercial-off-the-shelf (COTS): part of warranty and maintenance plan	Contract (Section 8.3)
TIH	Maintenance	RedyRef	COTS: part of warranty and maintenance plan	Contract (Section 8.3)
PED-X	Operations	City of Buffalo (CoB)	Leveraging CoB resources: signal operations	MOU (Section 7.1)
PED-X	Maintenance	CoB	Leveraging CoB resources: signal operations maintenance	MOU (Section 7.1)
Call Center	Operations	VIA	Operate call center	MOU (Section 7.2)
Reservations, Scheduling and Dispatch (RSD) System	Operations	New York State Department of Transportation (NYSDOT)	Operate software for RSD Monitor to security	MOU (Section 7.4)

An enumerated set of roles and responsibilities, contacts, service level agreements for each of these systems are described in **Sections 7 and 8**.

3. Issues Management Process

3.1. Overview

The Issues Management Process provides a means to manage all issues, defects and anomalies that may occur during systems operations. The issues may be detected from any of the subsystems and components of the All Access System, including turn-key and contracted systems. Detection of the issues may arise from internal monitoring services or through

- User reporting via customer satisfaction surveys, comments, or the Call Center (CC)
- Operational managers
- System monitoring via alerts or other methods
- Reports to the Project Management Team

When reported to the management team, operational managers, or CC, the issue will be recorded in an issues log. When detected by a system operator (including external maintenance/operations), it will be included in the system's issues log and reported through their monthly Service Level Agreement (SLA) reports to the All Access Team.

When logged by the CC, the issue will be logged and assessed initially through the Frequently Asked Questions (FAQ) troubleshooting of the CC staff. They will log and open the issue and assign it to an organization (e.g., CoB for Miovision, Etch for All Access App, etc.). The Call Center will contact some responsible organizations directly when an issue arises, particularly operations related issues. These include:

- SDS shuttle
- NFTA (train, bus and on-demand shuttle)

The issues will be reviewed on a weekly basis during the Management Team meeting unless a critical or high priority issue is detected. The workflow and timeline for review is detailed in **Figure 2** and handled as described in the *Issues Management Work Flow* (**Section 3.3**).

3.2. Issue Categorization and Impact

The issue categorization will be based on the critical vs. non-critical nature of its impact. The issue ticket will be expanded to incorporate priorities related to safety and hardware elements. The issue ranking, described in **Table 4**, applies to all subsystems and components of the system. S1 and S2 issues are considered critical rankings and should be fixed within 72 hours to 1 week following detection. S3 and S4 will be completed and updated at the next code release or update cycle.

Table 4. Issue Categories.

Issue Rank	Priority	Description
S1	Critical	System is not responding; system outage or system malfunction poses safety risk. **Unscheduled downtime. Must be fixed immediately.**
S2	High Priority	Major component, feature or functionality within the system is not working. Causing a critical disruption for users. **Must be fixed immediately.**
S3	Medium to High Priority	Key defect or functionality that should be working in the short term (next release). **Will be incorporated into the next version or release.**
S4	Normal Priority	Issue in functionality that should be reported to appropriate developer, implementor or integration team to resolve such as color change. **Will be incorporated into the next version or release.**

3.3. Issue Management Work Flow

The issue management work flow is depicted in **Figure 2**. An issue is detected and logged into a Google Sheet available to all system operators, technical teams, and All Access project staff. The process flow includes the following states:

Detected: when an issue is detected or reported, it is logged into the Issue Log.

Open: when reviewed by a team of technical experts (issues review board), a ticket is opened to address the issue. The team assigns a priority ranking to the defect that includes a critical path or non-critical path. Determination of a critical vs. non-critical path is determined by the issue impact (see **Section 3.2**). The review may include a solution to the issue.

Assigned: after the issue is opened, the issue is assigned to a tech team and / or tester. The technical team lead typically assigns the developer.

In-Progress: when the tech team begins working on the issue, the state is changed to in-progress. The state also includes completion and passage of all related test cases. Regression testing may be needed to approve the testing.

Closed: when the testing results are reviewed and confirmed by the Tech Leads, they are presented to the System Owner who closes the issue. The issue remains in a **Pending Close** state until the fixed version of the code is posted to the app stores or deployed in the field.

Cancelled: due to refactoring or other changes in system requirements or needs, the issue is obsolete, no longer occurs or was misreported. The system owner must agree that the issue is abandoned. An issue will be cancelled if one of the following assessment results is true:

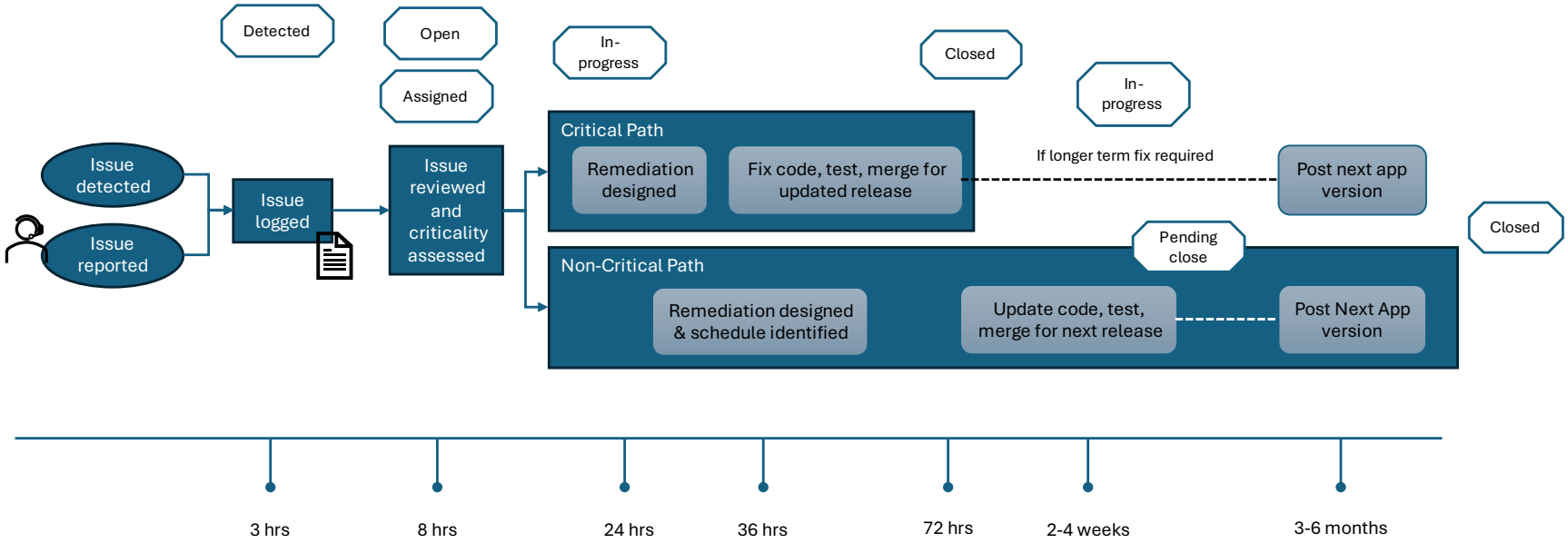
- The issue cannot be reproduced and there is no impact on any of the systems.

- The issue is duplicated by another defect. Additional details of this report should be transferred to the other issue report.
- The issue is determined to be a user error. Information on this report will be forwarded to training staff.

Reopened: if an issue occurs again once closed, the tech team may reopen the issue item.

Note that the Cancelled and Reopened states are not included in the Issues Management Process Flow diagram.

Each subsystem and component element handles their in-progress remediation and recovery processes differently. These are described in each Section (i.e., Section 4 for Buffalo All Access App and Section 5 for PMD). Furthermore, when the issue is assessed, the remediation timeline will be updated based on the critical path vs. non-critical path process. The timeline depicted in **Figure 2** is a worst case duration for critical path issues.



Issues Management Process

Figure 2. Issues Management Process.
Source: Buffalo, NY ITS4US

3.4. Issues Log Format

The issues log is designed as a form that adds a line to a Google Sheet when it is submitted. The Google Sheet will include the fields described in **Table 5**. The enumerated types included in the Type field include the following:

1. Commendation
2. All Access App
3. All Access Mobile app
4. All Access Web app
5. Community shuttle
6. Automated shuttle
7. NFTA on-demand shuttle
8. Indoor Navigation at VIA
9. Indoor Navigation at BGMC
10. Signal at Best / Main
11. Signal at Ellicott and High
12. Kiosk at NFTA
13. Kiosk at BGMC
14. Other

Table 5. Issues / Complaints / Commendations Report Template

Field	Form Mandatory / Optional	Format	Description
Date/time	Autogenerated	Date/time	Date and time issue was recorded
Person Entering Entry	Autogenerated	Free Text	Name of person entering text through form (check box if adding email address)
Name	M	Free text	Name of person issuing commendation or complaint
Email	O	Email format	Email of person issuing commendation or complaint
Type	M	Enumerated	Complaint / Commendation, see enumerated list below
Commendation	O	Free text	If commendation, then add comments
Complaint description	O	Free text	Description of complaint
Add summary of issue and troubleshooting results	O	Free text	Summary of issue and troubleshooting results
Current Status	n/a	Enumerated	Status of the complaint (Logged, Assigned, In-progress, Cancelled, Suspended, Closed)

Field	Form **M**andatory / **O**ptional	Format	Description
Last Status Date Change	n/a	Date	Date when the current status was set
Reviewed by	n/a	Free Text	Person who changed the current status

The issues log will be maintained for the length of the deployment. It will be reviewed daily and downloaded monthly for tracking and archiving.

Note: the Google Form automatically records an unique index and email address for each entry. The form can only be accessed by call center agents, All Access vendors and team members. Contact Polly Okunieff (ICF) to request access to the form.

4. Buffalo All Access App

Operations and maintenance for the Buffalo All Access App includes a list of the configurable items (software and operating environment), operational and maintenance roles and responsibilities, operational and maintenance procedures.

4.1. Configurable Items

4.1.1. Software – Operational and Cloud

The software items that are used by the Buffalo All Access App and licensed to Etch are listed in **Table 6**.

Table 6. Software Items used by the Buffalo All Access App.

Type	Vendor	Estimated (# units / yr)	Reference
Cloud services	Amazon Web Services (AWS)	12 months	Section 4.1.1.1
Multifactor Authentication (MFA) via email	AWS	1,000	Section 4.1.1.1
MFA via telephone call	Twillo	50,000	Section 4.1.1.2
MFA via Short Message Service (SMS)	Twillo	30,000	Section 4.1.1.2
Chat Bot	Open AI	36,500	Section 4.1.1.3

4.1.1.1. Cloud Services and Security Services

The cloud services used by the All Access App include the following AWS suite of products:

- AWS Amplify: Approx $0.50 / month
- AWS Dynamo: Approx $0.50 / month
- AWS Lambda: Approx $0.05 / month
- AWS API Gateway: Approx $20 / month
- AWS Web Application Firewall (WAF): Approx $6.50 / month
  - This includes the email service provider (ESP) for MFA via email
- AWS CloudWatch: Approx $20 / month
- AWS Elastic Container Registry (ECR): Approx $2 / month
- AWS Elastic Kubernetes Service (EKS): Approx $110 / month

Because the implementation is scalable (e.g., using microservices), the approximate load and service resources are flexible and depend on usage.

The cloud services are procured using an annual license and procured by Etch but will be transferred to the product owner at the end of Phase 3.

4.1.1.2. Multifactor Authentication Services for SMS and Telephone -- Twilio

Twilio (twilio.com) provides API tools to implement user authentication using telephone and SMS MFA methods. The license uses the pay-as-you-go pricing model. The tools used include:

- SMS –send and receive SMS and MMS messages ($0.0079)
- Voice APIs – enable calling into any application ($0.0089/min)

Anticipated resources used are shown in **Table 6**.

4.1.1.3. ChatBot

The All Access App uses OpenAI ChatGPT to build a scheduling assistant that converts speech to text. The system uses the GPT 4o API.

Version: GPT 4o API (https://platform.openai.com/docs/models/gpt-4o)

Resources: pay as you go model

4.1.2. CTP Software (All Access App)

The design of the CTP software is detailed in the SDD Section 4.

At the end of Phase 2, the code and build routines will be stored at GITHUB sites:

- https://github.com/etchgis/ctp-app
- https://github.com/etchgis/complete-trip-web
- https://github.com/etchgis/ctp-otp

Operations and Maintenance Roles and Responsibilities

Operational and maintenance roles and responsibilities for the CTP software are listed in **Table 7**.

Table 7. Operational Roles and Responsibilities

Role	Organization	Responsibilities
Software Administrator	ETCH	• Manage issues desk • Monitor security logs • Ingest external data including General Transit Feed Specification (GTFS) updates from NFTA and Community Shuttle • Monitor automated backups and when necessary, perform manual backups • Implement security management plan when necessary • Conduct system restoration if major failure occurs
Bridge/Middleware Application Programming Interface (API)	ETCH	• Maintain middleware (bridging) APIs when CXApp INS SDK is updated
All Access App mobile and server software	ETCH	Maintain software including: • Update patches based on operating system (OS) software updates and security patch • Manage issues for code including critical vs. non-critical issues • Enhance app software when directed • Manage CTP GitHub site • Update documentation for CTP based on updated software

4.2. Operations Procedures

This section includes the operational procedures including the modes of operations, operational processes, issues handling procedures, and shutdown/restart/recovery procedures.

4.2.1. Operational Modes

The All Access App Modes of Operations are described in **Table 8**.

Table 8. All Access App Modes of Operations

Mode	Definition
Normal Operations	All interfaces and subsystems are operating normally.
Degraded – external interfaces	This mode occurs when external interfaces are degraded or fail due to communications or data feed reduced availability, maintenance or other impacts.

Mode	Definition
	When the App identifies that data on which it depends is not verified, accurate or fails, the App will revert to static information and alert travelers about the degradation, i.e., the data is based on schedule data. The interfaces will revert to their independent component mode of operations, for example, the pedestrian crossing requests will rely on manual actuation. The impact is minor since there is still schedule information available on the App. The App indicates that the data is scheduled (vs. real time) and/or functions are still available for PED-X. Impact Low.
Degraded – Community Shuttle interfaces	This mode occurs when community shuttle reservations interfaces are degraded or fail due to communications or data feed reduced availability, maintenance or other impacts. The specific shuttle service will not be active on the App. If this a system-wide communications outage (and both on-demand and automated shuttle services are out-of-service), the App will not operate on any traveler's mobile or web platform. The impact is medium since there are other services that can replace the service that is not operating. For example, if the SDS shuttle is inoperable for maintenance, then the on-demand service will be available for mobility services. Impact Medium.
Degraded – TIH not working	This mode occurs when the TIH is not working properly, the controls are not available (e.g., accessible), or other functional issue. The impact is low since there are other services including the Call Center that the traveler may use to plan a trip or access mobility services. Impact Low.
Degraded – persistent error	This mode occurs when there is a persistent error in the App, for example, the system changes the traveler's profile, or the indoor navigation function does not recognize the facility. Impact High -- when the persistent error impacts the traveler's trip plans. Impact Low -- when the persistent error impacts preferences or App user experience
Failure	Failure mode operates as a mission critical impact. Information provision, communications and services between systems will be manually implemented. If no backup or redundant service is available, the operations will be suspended temporarily. Impact Critical.

4.2.2. Operational Processes

The operational processes include both automated and manual processes and tools that are used to operate and ensure the currency of the system.

4.2.2.1. Security and System Monitoring

The system includes continuous automated processes for monitoring the system and ensuring securing PII.

- Monitoring CTP components and all their associated AWS resources.
- Encrypting all messaging in transit and ensuring security certificates remain up to date.
- Encrypting all data at rest.
- Keeping software dependencies up to date.
- Adjusting system and/or operation in response to published Common Vulnerabilities and Exposures.

Etch hosted solutions always use Prometheus (promettheus.io) and Alertmanager (open source monitoring module-- https://github.com/prometheus/alertmanager) to collect service metrics and send automated alerts to the whole-team Slack alerts channel. Developers see incidents within seconds of when they occur, for example if a Kubernetes worker node has exceeded 80% of available physical memory. The alert includes a link to the Graphana dashboard for visualizing the situation in multiple ways: work node condition, pod metrics, individual containers, and deployments.

Etch uses the Open Worldwide Application Security Project (OWASP) Top 10 for 2021 Guidelines (https://owasp.org/www-project-top-ten/) as a foundation for secure operations. Security monitoring is provided through the following measures:

- Frontend dependency vulnerabilities are identified by npm audit (https://docs.npmjs.com/auditing-package-dependencies-for-security-vulnerabilities).
- The ESP uses AWS WAF with the AWS managed ruleset which automatically applies OWASP Top 10 guidelines to identify and block violations and attempted exploits on the fly. The rules are continuously updated to provide broad protection as the threat landscape constantly evolves.
- Snyk (snyk.io) provides vulnerability scanning of code plus container images. It ensures that base images or other dependencies with known CVE will be quickly identified and replaced.
- Etch subscribes to Cybersecurity and Infrastructure Security Agency's (CISA) exploit news alert service for major emerging threats.
- Operating system updates are applied through AWS EKS worker node groups. As AWS releases updates to Kubernetes and base images, Etch recycles the entire node group to the latest AWS-managed operating system image available. As system updates are made, the Kubernetes pods are shuffled onto new machines automatically.
- For the Lambda-hosted services (ChatBot, Travel Coordinator), AWS handles the updating of the underlying physical environment that Lambda functions execute within.
- The CTP architecture treats individual machines as expendable and does not attempt to update older machines, they are simply replaced. This architecture also provides automated fail-over as worker nodes are lost, as Amazon Auto Scaling Groups are used to automatically scale to increase load or recover from hardware failures.

- All worker nodes are in a virtual network with a private subnet that is not directly accessible from the internet. All outside communication occurs through the AWS Application Load Balancer protected by WAF.
- The platform is entirely cloud-hosted and accessed over the web or app store, and software will not be installed on personal computers of any users. This minimizes the exposure of private data to network intrusions such as ransomware encryption attacks and eliminates the need for users to manage application updates.
- System secrets are protected by Amazon's Key Management Service (KMS)
- AWS manages Secure Sockets Layer (SSL) certificate renewal.

4.2.2.2. External Data Updates

The system includes automated and manual data updates. Manual updates are triggered by alerts from external sources such as NFTA GTFS files. Automated updates are ingested as part of the normal system operations. These include: NFTA GTFS-realtime, OpenStreetMap, and the indoor navigation facility data.

4.2.2.3. Reliability and Performance Statistics

The system includes tools that gather and report on system performance and usage. These tools generate standard reports. They include:

- Google Analytics download on a regular basis
- Alertmanager to collect service metrics and send automated alerts to the whole-team Slack alerts channel

Uptime requirements, not including planned maintenance, will be documented and reported monthly. The target uptime per year will be 98% or no more than 7.3 days of unplanned downtime per year.

The reports are reviewed monthly with the project management team.

4.2.2.4. Backup and Recovery Processes

The system provides continuous backup services of the App user information. Amazon DynamoDB provides point-in-time recovery (PITR), which is a continuous backup technology that allows the database to be rewound to a past time. The backup goes 35 days back.

The software exists as versioned Docker images in Amazon ECR. It is possible to point to past Docker image version numbers in order to switch to older versions of the software. When servers fail or restart, they automatically pull the image corresponding to the deployed version number.

AWS DynamoDB backup service documentation is available at https://docs.aws.amazon.com/dynamodb/.

4.2.3. Security Management Plan

The Security Management Plan complies with the provisions of the NFTA Security Incident Response Standard and Plan (document is not publicly available) and the Buffalo Project Privacy Management Plan. If a breach or security risk is identified in the Buffalo All Access App, the Etch team will detect it during its daily security review and alert the NFTA cybersecurity team representative to advise on the procedures

which they will implement at detection, response and after-action periods. The current contact for the Etch team is Robert Jones, NFTA Deputy Director or designated staff. Any incident must be reported within the hour of detection.

The procedures to report to NFTA include:

(1) who needs to be contacted when a breach occurs;
(2) the actions followed after the breach occurs including periodic communications updates;
(3) laws that need to be followed in such cases;
(4) mitigation strategies to minimize the impact of the breach; and
(5) after-action analysis to identify the cause of the breach, how current procedures can be improved, and how to guard against it occurring in the future.

4.2.4. Operational Issue Handling Procedures

Operational issue handling procedures will be implemented following an issue that is identified as an All Access App issue. The App operational issues handling procedures are initiated following the “in-progress” state of the IMP.

Handling of the issue will follow an Agile approach similar to applied during the development process. When a non-critical issue is identified, a ticket will be developed, and it will be scheduled during the Agile Planning meeting. A critical or high priority ticket will be addressed immediately.

A critical or high priority ticket will be assigned to a developer; the developer will recommend a remedy to the issue; the issue will then be fixed. If the solution cannot be implemented within 72 hours, a temporary fix may be recommended (e.g., due to changing vendor API or refactoring code), with a longer-term solution identified for a later implementation. The temporary solution will need to provide normal mode of operations to the extent that is possible.

4.3. Maintenance Processes

Maintenance processes include the following:

- Software updates due to operating system updates
- External interface changes
- App remediation for critical and high priority issues
- App version release
- Infrastructure updates by cloud services (i.e., AWS)

A software change bulletin is issued when an updated version of the software is published to the app store.

4.3.1. Software Update Process

The software update process is implemented using an Agile approach. Decisions and schedules to update the software depend on the criticality of the change. The categories include those listed in **Table 9**.

Table 9. Software Update Type and Criticality

Change Type	Description	Actions / Criticality
OS security patch	A notice and software update published by the OS manufacturer describing a security gap in their operating system.	Developers will assess the impact on the system and update the code as necessary. This may require that the code be updated. Criticality: high priority
OS version update including mobile app native SDK update	A notice and software update published by the OS manufacturer describing an update to the underlying changes to the OS and/or SDK.	Developers will assess the impact on the system. If the updates do not directly impact the code, the update may be scheduled to be included in a later version update. Criticality: • Critical impact if directly impacts app functionality • Normal impact if the change does not directly impact app functionality
Critical and high priority ticket	A failure or defect in the app that requires remediation	Requires operational and issues handling processes to update the code within the SLA time period. Criticality: high priority
Medium to normal priority ticket	An issue or anomaly in the app that can be scheduled for the next release.	Schedule in the system backlog to update the issue and close the ticket. Criticality: normal priority
Enhancement to existing software	An enhancement to the code – either a change in user experience or added functionality.	Concurrence by project leadership and stakeholder request are needed to enhance the functionality. In addition, an estimate of the resources is also required. Criticality: normal priority

Every change will follow the Agile process described in **Figure 3.**

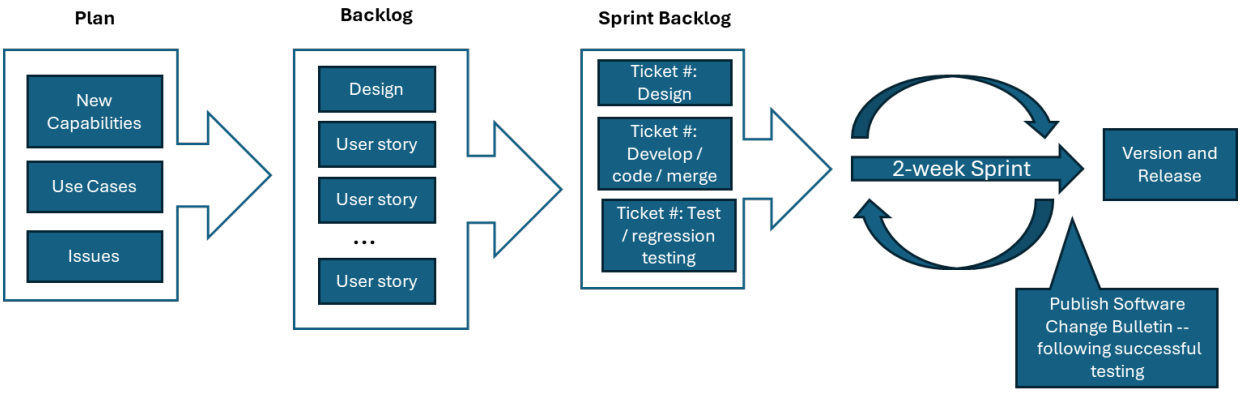


Figure 3. Software Change Process.
Source: Buffalo, NY ITS4US

4.3.2. Software Change Bulletin Process

A software change bulletin will be issued at least two weeks prior to releasing new versions of the App code. The bulletin will include the following information:

- Change Title
- Change Effective Date
- Version
- Change Description
- Reason for Change
- Impact of Change

The bulletin will be approved by the Project Manager prior to its publication and distribution. The changes will be provided to the app store and posted on the code repository and project website.

5. Performance Measurement Dashboard

Operations and maintenance for the Buffalo PMD includes a list of the configurable items (software and operating environment), operational and maintenance roles and responsibilities, operational and maintenance procedures.

5.1. Configurable Items

5.1.1. Software – Operational and Cloud

The software items that are used by the Buffalo All Access App are listed in **Table 10.**

Table 10. PMD Operational Software

Type	Vendor	License or Estimated # units/yr	Reference
Survey Monkey	SurveyMonkey	Advantage Annual	https://www.surveymonkey.com
Mail Chimp	Mailchimp	Essentials Month	http://mailchimp.com
shinyapps.io	Posit	Professional License Annual by RSG	https://www.shinyapps.io/
RStudio	Posit	Open Source Edition	https://posit.co/products/open-source/rstudio/

5.1.1.1. Survey Monkey

Survey Monkey is an online platform for surveys and forms. Buffalo All Access uses Survey Monkey to create and administer online surveys through a Survey Monkey account that is only accessed via the UB secure server. Survey links will be sent to participants through Mail Chimp. The license used for this project is the Advantage Annual subscription plan which allows to create unlimited survey questions, export data in csv, pdf and ppt file formats, and add custom logo and survey URL so that an authorized PMD team user can customize the pre-deployment and post-deployment surveys as needed.

5.1.1.2. MailChimp

MailChimp is an email marketing and automations platform to send survey links to Buffalo All Access participants. The software offers tracking survey responses by email addresses and sends reminders only to participants who haven't completed the assigned surveys. The license used for this project is the Essentials plan, the lowest MailChimp subscription tier that offers the functions this project needs. This account will only be accessed via the UB secure server.

5.1.1.3. Shinyapps.io

shinyapps.io is a shiny-based app hosting medium that the Buffalo Access PMD dashboard uses. It hosts each app on its own virtualized server. shinyapps.io is secure-by-design. Each app runs in its own protected environment and access is always SSL encrypted. It does not require developers to own a server or know how to configure a firewall to deploy and manage the app in the cloud. shinyapps.io is currently hosted on AWS infrastructure. The PMD dashboard is hosted under RSG company account.

5.1.1.4. RStudio

RStudio is an integrated development environment (IDE) for R and Python. It includes a console, syntax-highlighting editor that supports direct code execution, and tools for plotting, history, debugging, and workspace management. It is used for the development of data processing and PMD dashboard scripts, as well as deploying the shiny app to shinyapps.io.

5.1.2. PMD Software

The PMD software design is described in SDD Section 6.2.1 Survey Processing. The code uses R for input data processing and dashboard development using RStudio as the IDE. The code is stored in, https://github.com/RSGInc/Buffalo_pmd, a public GitHub repository site (see Figure 4). Any data that is stored on the site is Personally identifiable information (PII) free.

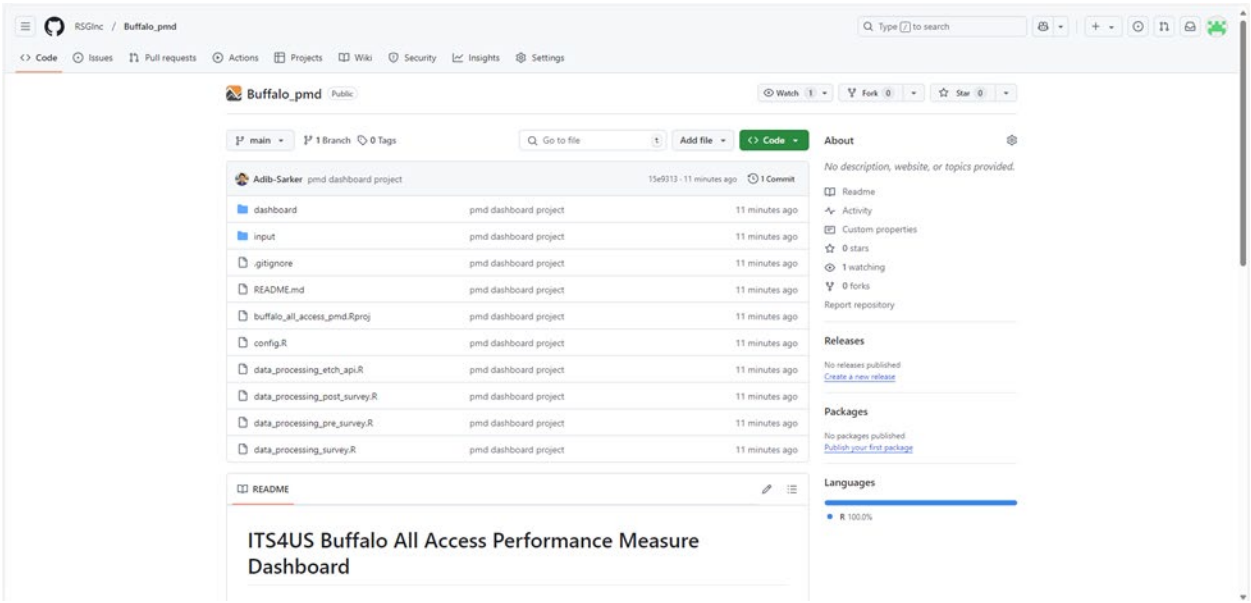


Figure 4. Public PMD GitHub Site

5.2. Operations and Maintenance Roles and Responsibilities

Operational and maintenance roles and responsibilities for the CTP software are listed in **Table 11**.

Table 11. Operational Roles and Responsibilities.

Role	Organization	Responsibilities
UB Server Administrator	UBIT	These responsibilities are part of the University at Buffalo / IT Department's existing services and procedures. • Operations of the server • System security monitoring and mitigation procedures ○ Enforce Security Management Plan which covers all UB servers • Role based access and authentication • Backup and restoration of system
Data Manager	RSG	• Curate periodic data updates from subsystems and components (in UB server) • Manage data recovery when data is lost • Remove data (especially PII) after 3 years.
PMD Dashboard Administrator	RSG	• Operations of RShiny dashboard • Generation of monthly metric reports • Management and configuration of analysis software • Load new metrics to PMD
Survey Processing Manager	RSG / UB	• Post, open and close survey • Ensure survey was included in Institutional Review Board (IRB) compliance • Update and compile survey data
IRB Compliance Manager	UB	• Ensure that all recruiting and evaluation materials have been submitted and approved by the IRB
PMD Dashboard Software Maintenance Manager	RSG	• Update software based on changes to external interfaces or ingestion of new data • Address and update software based on issues and anomalies • Update documentation based on updates • Enhance software to augment dashboard • Manage PMD GitHub site

5.3. Operations Procedures

This section includes the operational procedures including the modes of operations, operational processes, issues handling procedures, and shutdown/restart/recovery procedures.

5.3.1. Operational Modes

The PMD of Operations is described in **Table 12**.

Table 12. PMD Modes of Operations

Mode	Mode Definition / Impact
Normal Operations	All interfaces and subsystems are operating normally.
Degraded – data ingestion	This mode occurs when the data curation process is disrupted, or data is corrupted, missing or of low quality. Without the data, the metrics will not be updated. An investigation related to the missing data will be undertaken and recovery procedures will be put in place. Impact Low – metrics may be delayed for a period, but once recovery is initiated, the metrics may be updated, or a gap will be identified in the metadata.
Degraded – persistent error	This mode occurs when there is a persistent error in the PMD, for example, the file download. Operational issue handling procedures will be implemented to address the error. Impact Medium -- when the persistent error impacts the generation or presentation of metrics. Impact Low -- when the persistent error impacts access to PMD data.
Failure	Failure mode operates as a mission critical impact. Information provision, communications and services between systems will be manually implemented. If no backup or redundant service is available, the operations will be suspended temporarily. Impact Critical.

5.3.2. Operational Processes

The operational processes include both automated and manual processes and tools that are used to operate and ensure the currency of the system.

5.3.2.1. System Monitoring

The following systems will be monitored by the appropriate administrator. Automated services are embedded in the software to alert the administrator to issues that might arise. **Table 13** lists the system component and description and the actions addressed by the appropriate system administrator.

Table 13. System Monitoring Activities

System Component / Administrator	Description	Action Required
Dashboard / PMD Admin	Reliability: PMD dashboard is working online. Capacity (storage): Check the size of PMD input data (surveys and CTP trip files).	In general, shinyapps.io has 99.92% uptime, Posit Status. If the dashboard is down (reported by users or PMD team), PMD team will use a premium email support that responds to the questions within 24 to 48 hours. Capacity – If wrong (large) input files, especially CTP trip data were identified, PMD team will reach out to Etch to check the CTP trip data and push it again with the correct one.
Survey / Survey Processing Admin • SurveyMonkey • MailChimp	Reliability: SurveyMonkey link is not working. MailChimp software is not working. Capacity (storage): Not relevant	SurveyMonkey is one of the main online survey platforms widely used in industry. They provide daily incidents report online but show mostly no incidents reported. In case of the link down, PMD team will reach out to SurveyMonkey 24/7 priority email support. MailChimp is owned by Intuit and offers a reliable service. Based on their uptime report status, it offers 99.99% service operation status (see Mailchimp Server Status). If the service is not working, PMD team will wait half a day to see if it is back. If not, the team will use 24/7 email & chat support to fix the issue.

5.3.2.2. Back up Processes

Backup is performed daily. The UB server is backed up every night. A report is generated each morning showing the results. All backup, recovery and restore functions are performed by the UBIT. Information for requesting backup, recovery and restoration services is available from: https://www.buffalo.edu/ubit/services/all/data-backup-and-restore.html,

5.3.2.3. Performance Data Curation

Frequent monitoring of performance data curation will be undertaken by RSG developers (see **Figure 5).** The RSG team will review and conduct quality checks on the survey data collected through SurveyMonkey and CTP data collected via data push to the UB secure server by Etch. This will be done as part of a weekly data update to the PMD dashboard, keeping all stakeholders informed about the status of data collection. Automated metadata update, which will be visualized on the dashboard, will also be performed.

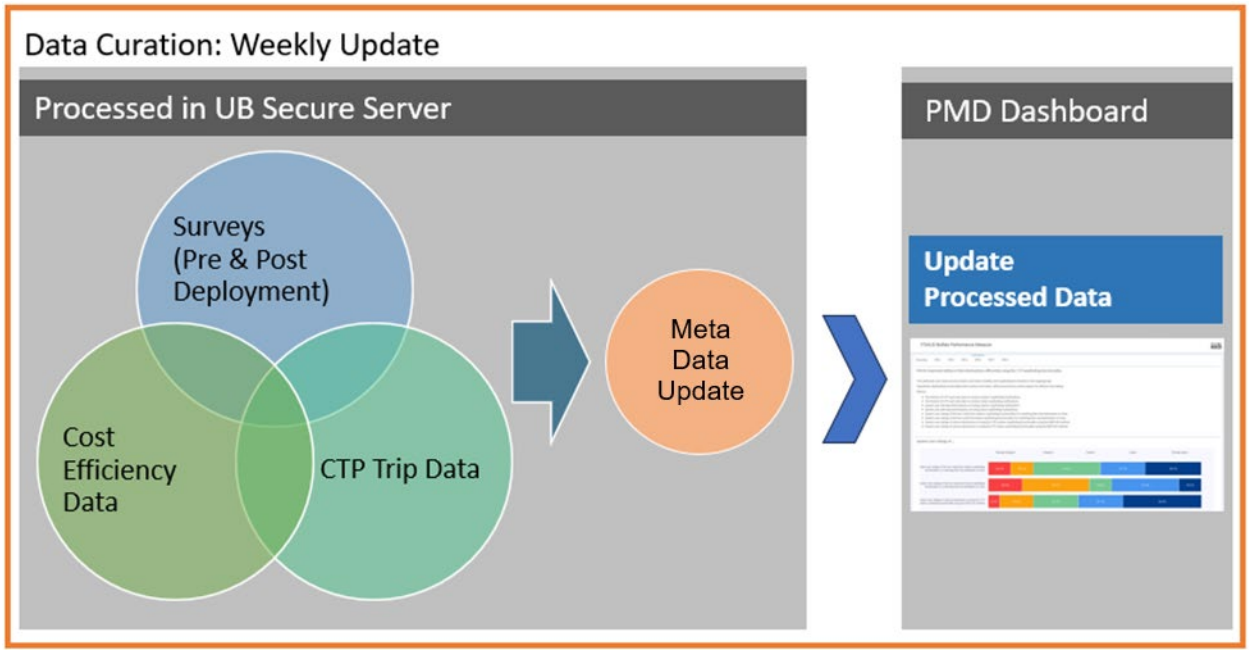


Figure 5. Weekly Data Curation Processes

5.3.3. Operational Issue Handling Procedures

Operational issue handling procedures will be implemented following an issue that is identified as a PMD issue. The PMD issues handling procedures are initiated following the “in-progress” state of the IMP.

Handling of the issue be handled based on a priority ranking.

A critical or high priority ticket will be assigned to RSG developer; the developer will recommend a remedy and the issue will then be fixed. If the solution cannot be implemented within 72 hours, a temporary fix may be recommended (e.g., due to changing vendor API or refactoring code), with a longer-term solution identified for a later implementation. The temporary solution will need to provide normal mode of operations to the extent that is possible.

5.3.4. Operations Shutdown, Restart/Recovery

This section describes the shutdown and then restart/recover processes if any failures arise that force a shutdown.

5.3.4.1. Operations Shutdown

In any case that the PMD dashboard (see **Figure 6**) needs to be down to handle operational issues, the RSG developer will convert the application visibility setting to ‘private’ in the shinyapps.io admin page, which blocks any public access to the app. It still allows the RSG developer and other authorized users to view the app while RSG developers fix the issues. RSG developers will post a backup page that alerts the user that the page is temporarily offline.

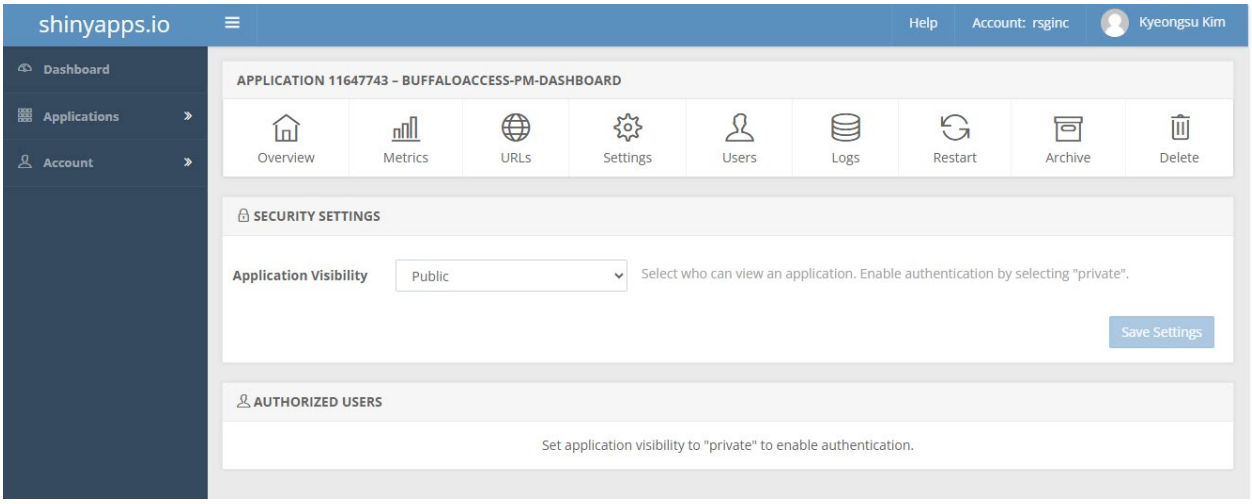


Figure 6. Administration Dashboard for shinyapps.io

5.3.4.2. Operations Restart/Recovery

After the issues are resolved, RSG developers will re-publish the app in the shiny dashboard development IDE (RStudio) and change the visibility setting to 'public' in the shinyapps.io admin page (see **Figure 7**). It allows the updated PMD dashboard to be visible to the public.

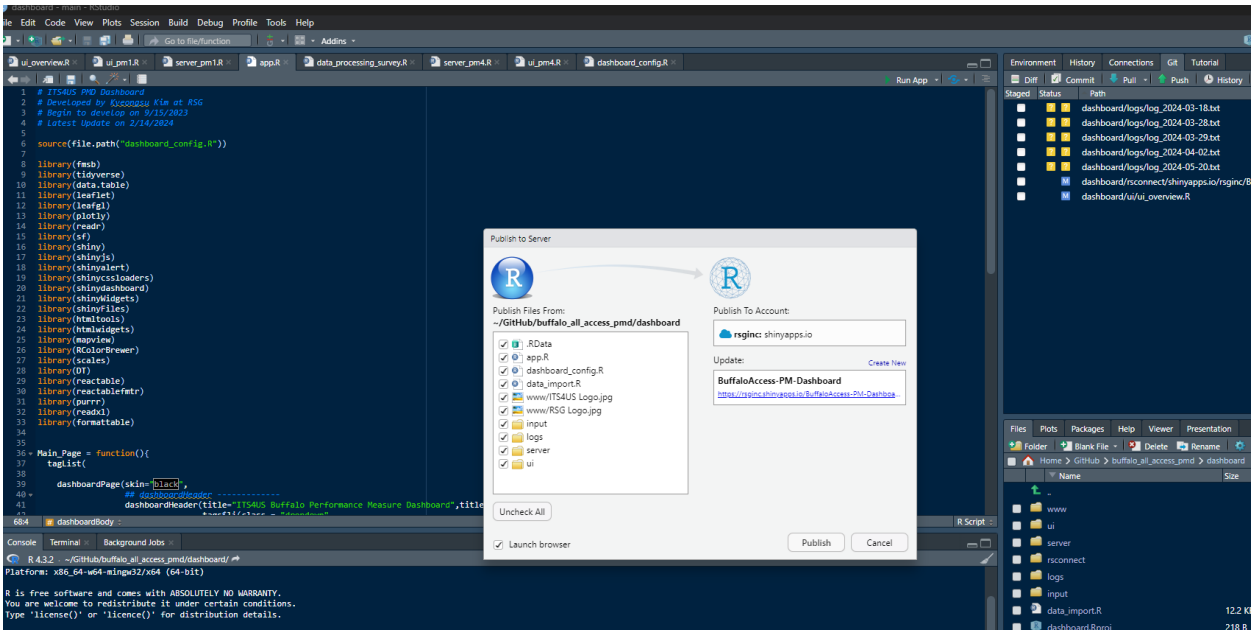


Figure 7. RStudio Recovery Dashboard

5.4. Maintenance Processes

Similar to **Section 5.3.4**, the PMD dashboard will be down for any major maintenance-related issues by converting the application visibility setting to 'private' in the shinyapps.io admin page. After the issues are resolved, RSG developers will re-publish the app via RStudio and change the visibility setting of the PMD dashboard to 'public' to be visible to the public.

No major or minor maintenance processes are anticipated for maintaining the PMD through the end of Phase 3. If infrastructure operating updates or versions impact operations, then the procedures outlined in **Section 5.3.4** will be implemented.

6. Operations and Maintenance Risks and Contingencies

Operational and maintenance risks apply to all the subsystems and their integration. The IOO deployed systems including CoB signal systems and NFTA on-demand shuttle services have redundant systems and risk contingencies to manage their risks; the SDS does not, and it is subject to risks for that do not apply to the on-demand shuttle. Hence this Risk Management Matrix (**Table 14**) only covers Buffalo All Access App and related components, as well as the SDS.

Table 14. Operational and Maintenance Risk Matrix.

Risk #	Component/ Subsystem	Risk	Contingency
001	All	System-wide issue such as power outage or communications issue	System cannot work without power and communications (e.g., internet, phone, MFA)
002	All	Weather impacts such as flooding, snowstorms, etc. • Staff cannot get to their posts • Safety issue with operations of community shuttle	System will be shut down until it is safe to travel.
003	Component (INS, kiosk)	Vendor goes out of business	Perform an alternative technology assessment to determine if there are other vendors using similar functionality / interfaces.
004	All Access App	Critical shut down or crash system	Apply Incident Management Process to identify a remediation approach during the interim. Generate message on the app to announce shut down.
005	All Access App	Critical issues that do not crash system	Apply Incident Management Process to identify a remediation approach during the interim. Identify and remove issue (or feature) that is crashing system until a fix is identified and in place.
006	All Access App	PII exposure	Implement security breach protocols

Risk #	Component/ Subsystem	Risk	Contingency
007	All Access App and External Systems	External API failures and impact on All Access App	Certain services provided to travelers through the App rely on the ability of external systems to produce that service. For example, the App relies on various APIs, e.g., NFTA bus and rail. If those external systems undergo unplanned failures or degraded service, the App will not provide travelers with services, which could lead to adverse perceptions from community members. The project team will work with external systems to mitigate this risk by coordinating service-level agreements and strategies for monitoring and notification in case of service disruption

7. Memorandum of Understanding with Stakeholder Partners

7.1. CoB Roles and Responsibilities

A project collaboration agreement was shared between the City of Buffalo and NFTA on January 16, 2024, which includes effective dates continuing through the end of the Buffalo, NY ITS4US project Phase 3 (if approved by USDOT) and the demonstration period. The Roles and Responsibilities associated with the agreement are listed in **Table 15**.

Table 15. City of Buffalo Roles and Responsibilities

Role	Organization	Responsibilities
Miovision Cameras	COB	Equipment and Logistics • COB will take ownership of 2 Miovison cameras (“equipment”) purchased by the Buffalo Niagara Medical Campus (“BNMC”), Inc. with federal funding under the ITS4US program; • COB will provide for all costs of installation, normal operations, and maintenance of the cameras during the ITS4US project Phase 3 (if approved by USDOT) and the demonstration period; • BNMC, Inc., through federal funding from the ITS4US program, will provide for any installation, operations, and maintenance costs that are directly related to the integration for the full trip application; • The programming will be limited to a read only state – the application will not have any access to alter the traffic signal timing; • COB will connect the equipment to its current Miovision dashboard for data collection and provide the Greater Buffalo Niagara Regional Transportation Council (“GBNRTC”) with access to data pertinent to grant objectives for analysis.

7.2. VIA Roles and Responsibilities

A project collaboration agreement, effective on January 1, 2024 and continuing through the end of the Buffalo, NY ITS4US project Phase 3 (if approved by United States Department of Transportation (USDOT)) was entered between the Buffalo Niagara Medical Campus, Inc. (BNMC), a New York State 501-c-3 non-profit corporation and VIA, a 501-c-3 non-profit corporation. The Roles and Responsibilities associated with the agreement are listed in **Table 16**.

Table 16. VIA Roles and Responsibilities

Role	Organization	Responsibilities

VIA Call Center	VIA	Equipment and Logistics
		• Provide a workstation (maybe shared).
		• Provide telephone or Voice over Internet Protocol (VoIP) service with additional services for people with hearing loss.
		  ○ Offer a separate telephone number for the ITS4US travelers.
		  ○ Provide access to a language line.
		• Provide internet access.
		• Establish, maintain and monitor a designated email account for questions, complaints, and commendations.
		Training
		• Make staff available for training as appropriate.
		• Provide ongoing training to new staff assigned to project.
		Operations
		• Staff call center with trained personnel Monday - Friday, from 6:00 AM to 7:00 PM Eastern Time (ET).
		  ○ Include Spanish language reps or access to a language line.
		• Support travelers with the CTP services
		  ○ Support travelers to use, apply, and sign up for the CTP services.
		  ○ Support travelers to plan their trip itineraries and on-demand reservations and assist with navigation.
		  ○ Help travelers who are having trouble with their trips, including dealing with their on-demand services.
		  ○ Record and report complaints / commendations from callers.
		  ○ Help travelers use the different CTP user interfaces (mobile app, web application, kiosk).
		• Report call taker / software issues through an issues tracking tool.
		• Record and report traveler issues using a Customer Relationship Management (CRM) tool.
		• Develop processes/protocols to operate call center for the ITS4US project.
		• Provide operational performance measures to Project Team (to be agreed upon prior to Phase III).
		• Meet periodically with Project Team.

Role	Organization	Responsibilities
VIA Indoor Navigation	VIA	• Install and monitor indoor navigation beacons in public places at VIA. • Alert BNMC if beacons require battery or device replacement due to failures
Project Team Support for Call Center	BNMC	Training • Provide train-the-trainer training session and materials to staff in Phase 2. • Provide on-line user manual for some troubleshooting and user training. • Provide IRB training for staff. Tools (All Access App) • Provide access to the All Access App (CTP) software. • Provide access to All Access App mobile app. Operations • Operate web site used by call takers. • Respond to call taker requests / questions within 24 hours. • Troubleshoot issues raised by call takers as needed.

7.3. Kaleida Health Roles and Responsibilities

The Kaleida Health, at its BGMC effective May 25, 2023 through the completion of the Buffalo, NY ITS4US Project Phase 3 agreement includes a service agreement with BNMC. The Roles and Responsibilities associated with the agreement are listed in **Table 17**.

Table 17. Kaleida Health Role and Responsibilities

Role	Organization	Responsibilities
Buffalo, NY Project Team	BNMC	• BNMC shall purchase and acquire all equipment that is necessary for the execution of the Program that will be installed on the Kaleida Property. • BNMC shall hire any subcontractors that are necessary to successfully carry out the Program. • BNMC shall ensure that all subcontractors providing Services under the Program have access to the INS back-office assets including but not limited to, existing maps, routes, and waypoints, along with the relevant ClientID and Client Secret software programs. • Upon the expiration or termination of this MOU, BNMC shall remove all of the TIH kiosks, and BNMC shall be liable for the cost of the removal and for the cost of restoring the Kaleida Property after such removal.

Role	Organization	Responsibilities
Kaleida Service Manager	Kaleida	• Maintain, in good and working condition, the INS beacons and batteries related to the INS throughout the term of the Program. • Allow BNMC subcontractors providing Services under the Program to have reasonable access to the INS back-office assets including but not limited to, existing maps, routes, and waypoints, along with the relevant ClientID and Client Secret software programs. • Provide support for testing of the INS software application to be developed as part of the Program, including making Kaleida personnel available to conduct formal testing of the INS software as needed by BNMC. • Manage the layout, waypoints, and routes, as they relate to the Kaleida Property, within the INS software, to include alerting BNMC when or if any changes to the layout, waypoints, and routes at the Kaleida Property will be made and a timetable for the completion of any changes therein. • Supply both an internet connection and electrical connection for the TIH kiosk at a mutually agreeable location that has sufficient electricity and internet connectivity and oversee the electrical connection and ensure all safety protocols are followed thereto. • Provide data security provisions to protect any and all electronic communications related to the TIH kiosk. • Alert BNMC if it notices there is an issue with the TIH.

7.4. NYSDOT Agreement

The NYSDOT Agreement will be included in the Phase 3 Transition Plan.

8. Service Level Agreements for Contracted Service Level Agreements

8.1. SDS Master Operations Plan

Bus Operational Plan

University at Buffalo

BNMC BUFFALO NIAGARA MEDICAL CAMPUS

New York State Department of Transportation

ADASTEC Automated, Shared, Connected

VICINITY

NEW YORK STATE Department of Motor Vehicles

BUFFALO ITS4US DEPLOYMENT PROJECT

Bus Operation Plan

8.1.1. Contact List

Table 18 to **Table 20** provide contact information for the UB, BNMC, and ADASTEC Corp.

Table 18. University of Buffalo (UB)

Name	Title	Email
Adel W. Sadek	Professor	asadek@buffalo.edu
Chunming Qiao	SUNY Distinguished Professor	qiao@buffalo.edu
Stephen Still	Professor of Practice	sestill@buffalo.edu
Victor Paquet	Professor	vpaquet@buffalo.edu
Jordana Maisel	Associate Professor	jlmaisel@buffalo.edu

Table 19. Buffalo Niagara Medical Campus (BNMC)

Name	Title	Email
Jamie Hamann-Burney	Chief Strategy Officer	jhamann-burney@bnmc.org
Shania Julia Anunciacion	Planning & Program Manager	sanunciacion@bnmc.org
Maria Morreale	Director of Marketing & Strategic Communications	mmorreale@bnmc.org

Table 20. ADASTEC Corp. / Vicinity Motor Corp. Team – Responsible for providing the bus and operating the pilot.

Name	Title	Email
Dr. Ali Peker	CEO	ali@adastec.com
Cemre Kavvasoglu	Product Management Director NA	cemre@adastec.com
Berna Gür	Project Management Engineer	berna@adastec.com

8.1.2. Project Timeline, Details and Milestones

8.1.2.1. Introduction

The Buffalo All Access project team, led by the Niagara Frontier Transportation Authority (NFTA), in partnership with the Greater Buffalo Niagara Regional Transportation Coalition (GBNRTC), the Buffalo-Niagara Medical Campus (BNMC), and the University at Buffalo (UB), along with several other regional partners, is launching a groundbreaking initiative with the Buffalo ITS4US Complete Trip Deployment project. As part of this effort, ADASTEC Corp. will deploy one full-size, electric, Level 4 automated shuttle in the Buffalo-Niagara Medical Campus area.

The initiative aims to assess the effectiveness of advanced autonomous shuttle technology in enhancing mobility for underserved populations, such as the elderly and individuals with disabilities. The project will also evaluate how these shuttles can improve local transportation efficiency and safety. By integrating cutting-edge technology into the city's transit infrastructure, the initiative seeks to demonstrate the potential benefits of autonomous electric shuttles in increasing accessibility and streamlining transportation in high-density urban settings.

The Self-Driving Shuttle (SDS) will provide a demand-responsive service to the Buffalo All Access app registered users for trips in the vicinity of the BNMC. SDS operations, however, will be constrained to a pre-defined route of pre-selected streets that satisfy the SDS Operation Design Domain (ODD), and at pre-defined pick-up and drop-off locations.

8.1.2.2. Phases

The Buffalo ITS4US Complete Trip Deployment Project consists of three phases:

Phase 1: Concept Development

The development of mandatory and desirable system requirements, establishing the project foundation through feasibility studies, stakeholder engagement, and initial design.

- Driven and self-driving shuttles (SDS), focusing on SDS operation.
- Smart Infrastructure Subsystem: Provides wayfinding and navigation support.

Performance Dashboard Subsystem: Tracks and displays performance and safety metrics.

Phase 2: Design and Testing

This phase is dedicated to the deployment and testing of a single self-driving shuttle (SDS). Key tasks included selecting vendors, planning the site, conducting preliminary tests without passengers, planning routes, integrating the SDS with existing systems, evaluating performance metrics, and preparing for passenger service.

Phase 3: Operation and Maintenance

This starts after “Phase 2” and pending successful testing and USDOT approval, will last 18 months and includes launching passenger service for the study’s participants, and ongoing system evaluation and

refinement. The project aims to expand the service area, operate and maintain the system for at least 5 years, and assess its impact on transportation efficiency and safety.

The goals of this project include

- Connecting neighboring communities to the BNMC with improved transportation services.
- Enhancing local circulation and pedestrian safety in the BNMC area.
- Creating a model for accessible transportation that can be replicated regionally and nationally.
- Measuring the impact of these mobility enhancements.

8.1.2.3. Subsystems

- Complete Trip Platform (CTP): Manages trip planning and navigation operated by Etch
- Community Shuttle Subsystem: Offers on-demand transit operated by NFTA

8.1.3. SDS Components

The SDS Subsystem itself is made up of the following components:

1. An ADASTEC-Vicinity Lighting Vehicle: The SDS deployed for the Buffalo All Access project is NOT a retrofitted vehicle, but a ground-up factory fitted automated bus produced by VMC, which means that the drive-by-wire conversion is done by the producer and thus existed prior to deployment. The model is the Vicinity Autonomous Lightning EV. The powertrain is battery electric, with 252 kilowatt-hour (kWh) battery size with a 180-mile range. The bus can be charged with either a Level-2 AC charger or a DC charger. The seating capacity is up to 22 passengers and with three wheel chair positions.

2. SDS Shuttle Operations Center (SOC): Manages routing, scheduling, and vehicle tracking, and interfaces with the Complete Trip Platform (CTP).

Table 21 provides a list of stakeholders and a description of their roles.

Table 21. Project Stakeholders and Roles

Stakeholder	Description
ADASTEC Corp. / Vicinity Motor Corp. Team	The developer of the Autonomous Driving System (ADS), flowride.ai, the manufacturer of the Shuttle. The team is jointly responsible for the production of the vehicle and the integration of the sensors, the drive-by-wire system and the ADS. Following deployment and testing, ADASTEC is responsible for operating the SDS throughout Phase III of the project.
The University at Buffalo	Responsible for overseeing the deployment, verification and evaluation of the SDS, and coordinating ADASTEC's activities with the rest of the Buffalo-All-Access team.

Stakeholder	Description
Niagara Frontier Transportation Authority	The lead organization for the Buffalo All Access project. Primary responsible for deploying the Human-Driven Shuttle
Buffalo Niagara Medical Campus (BNMC)	The Buffalo All Access project is taking place on the BNMC. BNMC is responsible for project outreach and management.
New York State Department of Motor Vehicles	Responsible for ensuring the AV demonstration meets all requirements of NYS Law regarding the testing and deployment of AVs on public roads. The entity responsible for granting the project team the AV permit.
ICF	Responsible for the development of the Buffalo-All-Access app and working with ADASTEC on integrating the app with the SDS.

Rider Experience

The rider's experience is at the forefront of our automated bus pilot deployment, ensuring that each passenger enjoys a seamless, comfortable, and engaging journey. From the moment passengers board the bus, they are greeted by a modern, clean, and welcoming interior designed with their comfort in mind. The ADASTEC-Vicinity SDS is equipped with advanced infotainment systems that provide real-time updates on routes, schedules, and points of interest, and offer features such as audio recordings, automated announcements, and visual displays, enhancing the convenience and enjoyment of the ride. Safety features, including easy-to-reach emergency buttons and clear, multilingual safety instructions, provide peace of mind throughout the journey. ADASTEC's customer service team is always accessible via in-bus communication systems to assist with any inquiries or concerns, ensuring that every rider feels supported and valued. ADASTEC is committed to delivering a rider experience that is not only efficient and reliable but also elevates the standard of public transportation through innovative technology and exceptional service.

8.1.4. Operations Plan

While providing a demand-responsive service to the Buffalo All Access app registered users, SDS operations will be constrained to a pre-defined route of pre-selected streets that satisfy the SDS ODD, and at pre-defined pick-up and drop-off locations. Details are provided below.

8.1.4.1. Schedule

Initially, the SDS operating schedule will be from 8:00 am to 4:00 pm. The schedule is expected to be adjusted based on observed demand during Phase III.

8.1.4.2. Route Specifications

Figure 8 below shows the proposed route for the SDS. A detailed route risk assessment that focused on the SDS deployment route of the SDS. The risk assessment process resulted in categorizing the route segments into five categories, each category having a similar risk level and site characteristics. The study

also provided several recommendations aimed at reducing the risk of the SDS deployment and operations (details provided elsewhere).

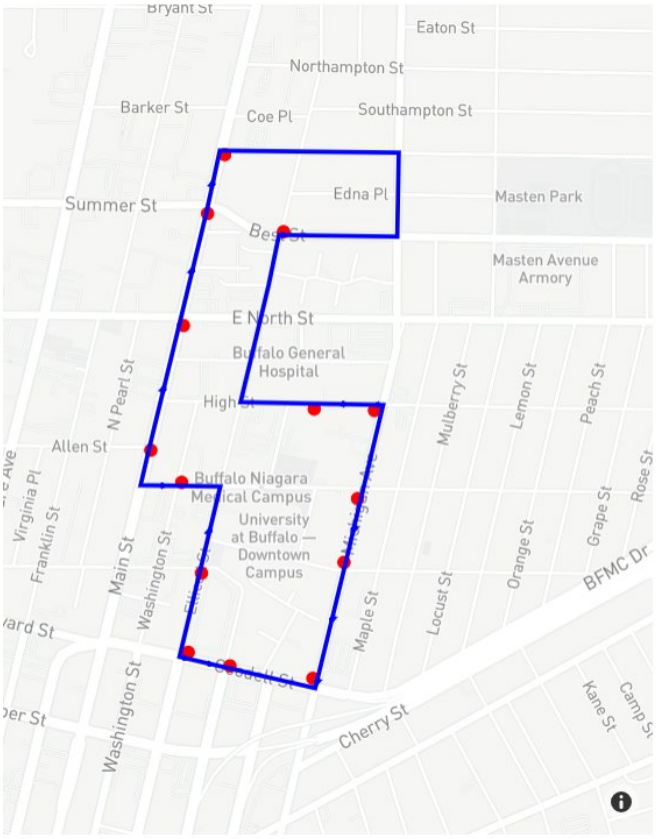


Figure 8. Proposed Route for the Self-Driving Shuttle
Source: University at Buffalo, 2024

8.1.4.2.1. Bus Stops

Figure 8 above shows the locations of the initial set of stops for the SDS (the red dots). These stops are co-located with the existing NFTA bus stops to ensure visibility and safety of operations. In addition, the Buffalo All Access team will identify an additional set of candidate locations, specifically for the SDS. This step is being performed in consultation with ADASTEC and the City of Buffalo.

8.1.4.2.2. Route and Stops

The route length is 2,86 miles. There are 17 traffic lights. Crowded Areas are parking areas, houses, a shopping mall, and a school. There are side and parallel parking places on the road. The max speed limit is 30 mph. The Shuttle will be operating in mixed traffic with vehicles, pedestrians and cyclists. A human safety steward will be on-board the bus all the time ready to take over manual control of the shuttle whenever necessary. All such instances of manual takeover (i.e., disengagements) will be recorded and analyzed to improve future performance.

8.1.4.3. Vehicle Staging, Storage, Charging

A facility located at 150 Myrtle Avenue in Buffalo, NY was secured for the SDS storage and charging. The facility provides year-round climate-controlled space for the parking and storage of the SDS, along with office and working space. The Buffalo All Access has installed a level 2 AC Charger with a capability of providing up to 18kwh, which will allow the battery of the SDS to be fully charged overnight. The facility was also equipped with internet access, a security system with 24/7 monitoring, a fire alarm and a CO monitoring system. **Figure 9** shows the floor plan for the SDS parking and charging facility.

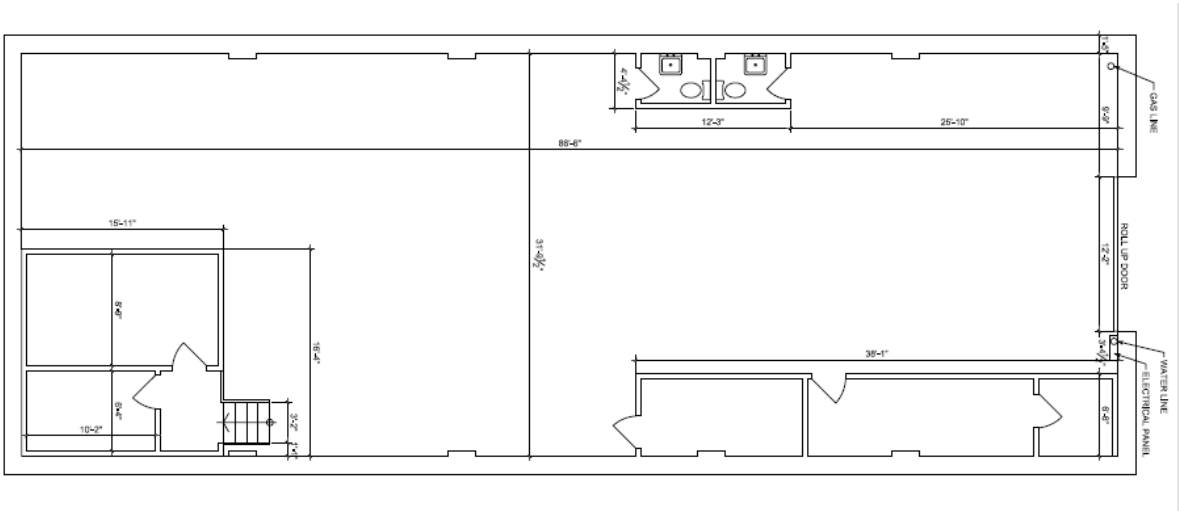


Figure 9. SDS Parking & Charing Facility Floor Plan
Source: University at Buffalo, 2024

8.1.5. Communication Plan & Safety Specifications

8.1.5.1. Physical Signages

To enhance the visibility and understanding of automated bus routes, it's suggested to implement effective physical signage on buses and at bus stops. This signage will provide crucial information to pedestrians, cyclists, and motorists about the presence of automated vehicle routes, ensuring a smoother and safer transportation experience.
Physical signages are necessary to raise awareness of pedestrians, cyclists, and motor riders that are on an “Automated Vehicle Route”. A sticker should be created to remind passengers to remain seated during the operation. A sample sticker is shown in **Figure 10**.

Figure 10. Sample Sticker for Reminding Passenger to be seated while SDS is moving
Source: University at Buffalo, 2024

The team will also be working with the City of Buffalo to create stickers intended to increase awareness for people, drivers, and riders near the SDS route, at bus stops. Sample stickers are provided in **Figure 11** and **Figure 12**.

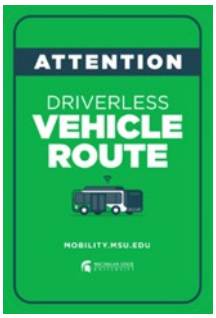


Figure 11. Sample Sticker to Increase Public Awareness of SDS Operations
Source: University at Buffalo, 2024

Figure 12. Sample Sticker for a SDS Bus Stop
Source: University at Buffalo, 2024

8.1.5.2. Safety Guidelines

The following Safety Guidelines shall be implemented on-board the SDS.

1. **Boarding and Seating:**
    - Only board the bus at designated stops.

- No standing passengers are allowed. All passengers must be seated while the bus is in motion.
- Fasten your seatbelt as soon as you are seated.

2. **Behavior and Conduct:**
   - No eating or drinking is allowed on the bus to prevent spills and maintain cleanliness.
   - Smoking and vaping are strictly prohibited.
   - Firearms and other weapons are not allowed on the bus.
   - Maintain respectful behavior towards other passengers and follow instructions given by bus staff or automated systems.
   - Avoid any disruptive behavior that could distract the automated systems or other passengers.
3. **Emergency Protocols:**
   - Familiarize yourself with the location of emergency exits and safety equipment.
   - In case of an emergency, follow the instructions provided by the automated system or bus staff.
   - Do not tamper with emergency equipment unless there is an actual emergency.
4. **Personal Belongings:**
   - Keep your personal belongings secure and store them in designated areas.
   - Ensure that aisles and exits are clear of personal items to avoid tripping hazards.
5. **Accessibility:**
   Wheelchair Accessibility: The bus is equipped to accommodate passengers using wheelchairs. Please inform the service provider of any wheelchair requirements at the time of reservation to ensure proper accommodation.
   - Wheelchair users must use designated spaces and securement systems provided to ensure safety during the journey.
   - Follow the instructions given by the bus staff or automated systems for proper boarding, seating, and exiting procedures.
6. **Health and Hygiene:**
   - Practice good hygiene and avoid traveling if you are feeling unwell.
   - Follow any health guidelines from the bus service providers, such as wearing masks if required.
7. **Compliance:**
   - Follow all local laws and regulations while using the bus service.
   - Adhere to the terms and conditions set by the bus service provider.
8. **Pet Policy:**
   - Pets, with the exception of service animals, are not permitted on the bus to ensure the comfort and safety of all passengers.

8.1.6. Crisis-Emergency Communication

A separate Incident Management Plan is being developed for handling emergencies and incidents related to the SDS. The plan will include step-by-step instructions on whom to contact in case of an emergency or SDS-related incident.

8.2. INS SLA

The indoor navigation system is a software as a service contract. The operations and maintenance of the system are governed by the contract between ICF International Inc. (ICF) and CXApp. Roles and responsibilities, issues management, and the terms of service are described in this section.

8.2.1. Role and Responsibilities

The roles and responsibilities associated with operations and maintenance of the INS SaaS are described in **Table 22**.

Table 22. INS Roles and Responsibilities

Role	Organization	Responsibilities
INS Administrator and Technical Assistance	CXApp	• Provide technical assistance • Manage portal • Update and enhance SDK; communicate updates to technical team • Manage beacon inventory and security settings
Contract Owner	ICF	• Oversee contract and audit service agreement • Facilitate communications between facility owners and CXApp • Facilitate communications between developers (Etch) and CXApp technical assistance

8.2.2. Issues Management Approach

If there is an issue with the INS native software or SaaS tools, the contract owner or technical team representative will send an email or call the INS contact person. Depending on the severity level of the issue, the CXApp contact will address the issue within a reasonable time (e.g., immediately for critical issues).

The contract owner or technical team representative will record the issue in the Issues Log and track it until the issue is closed.

8.2.3. Terms of SLA

The Service Level Agreement with the vendor CXApp is provided in **Appendix A**.

8.3. TIH SLA

The Transportation Information Hub (aka kiosk) includes a gold level service agreement (details follow in Service Level Agreement - Redyref). The operations and maintenance of the system is governed by the

contract between ICF and CXApp. Roles and responsibilities, issues management, and the terms of service are described in this section.

8.3.1. Role and Responsibilities

The roles and responsibilities associated with operations and maintenance of the TIH equipment and infrastructure software are described in **Table 23**.

Table 23. TIH Roles and Responsibilities

Role	Organization	Responsibilities
Kiosk Monitor and Administrator	RedyRef	• Gold level service agreement
Kiosk Maintenance Manager	RedyRef	• Troubleshoot kiosk maintenance issues (excluding WiFi, power, cleaning and vandalism • Replace equipment that malfunctions
Contract Owner	ICF	• Oversee contract and audit service agreement • Communicate with NFTA and Kaleida regarding issues that occur • Basic troubleshooting and periodic maintenance (e.g., cleaning) based on Owner's Manual (see **Appendix C**)

8.3.2. Issues Management Approach

Basic troubleshooting involves simply power cycling the Kiosk with the power button and possibly the monitor. All components and power supplies are labeled in the unit. Any assistance needed further than that, should be reported at support@redyref.com.

Depending on the severity level of the issue, the RedyRef contact will address the issue within a reasonable time (e.g., immediately for critical issues).

If RedyRef detects an issue with the kiosk through their on-going monitoring tools, they will send an email or call the contract owner with information on the issue or anomaly (depending on the severity of the issue). The contract owner or technical team representative will record the issue in the Issues Log and track it until the issue is closed.

8.3.3. Terms of SLA

The Service Level Agreement with the vendor Redyref is provided in **Appendix B**.

9. Reference Documents

The references provide additional information related to this document.

[1] [ConOps2] *Nayel Urena Serulle (ICF), et al (2024). Phase 1 Concept of Operations (ConOps) – Buffalo NY ITS4US Deployment Project, Phase 2 Update (FHWA-JPO-21-860).* Federal Highway Administration.

[2] [SyRS2] Polly Okunieff (ICF), et al (2024). *Phase 1 System Requirements Specification (SyRS) – Buffalo NY ITS4US Deployment Project, Phase 2 Update (FHWA-JPO-21-883).* Federal Highway Administration.

[3] [DMP2] Sadek, Adel W, et al. (2023). *Phase 2 Data Management Plan (DMP) – Buffalo, NY ITS4US Deployment Project (FHWA-JPO-22-973)*. Federal Highway Administration.

[4] [DPP] Sadek, Adel W., et al. (2023). *Phase 2 Data Privacy Plan (DPP) – Buffalo, NY ITS4US Deployment Project (FHWA-JPO-22-969)*. Federal Highway Administration.

[5] [PMESP2] Bradley, M., et al. (2024) *Phase 2 Performance Measurement and Evaluation Support Plan – Buffalo, NY ITS4US Deployment Project (FHWA-JPO-21-878)*. Federal Highway Administration.

[6] [SAD] Okunieff, P., et al. (2023). *Phase 2 System Architecture Document (SAD)* – Buffalo, NY ITS4US Deployment Project (FHWA-JPO-22-981) Federal Highway Administration.

[7] [ICD] Okunieff, P., et al. (2024). *Phase 2 Interface Control Document* – Buffalo, NY ITS4US Deployment Project (FHWA-JPO-22-981) Federal Highway Administration.

[8] [CAP] Okunieff, P., et al. (2022). *Phase 2 Comprehensive Acquisition Plan (CAP)* - Buffalo, NY ITS4US Deployment Project. Federal Highway Administration.

[9] [CIP] Okunieff, P., et al. (2022). *Phase 2 Comprehensive Installation Plan (CAP)* - Buffalo, NY ITS4US Deployment Project (FHWA-JPO-23-991) Federal Highway Administration.

[10] [SDD] Okunieff, P., et al. (2024). *Phase 2 System Design Document (SDD)* - Buffalo, NY ITS4US Deployment Project (FHWA-JPO-23-999) Federal Highway Administration.

10. Acronyms and Abbreviations

Table 24 summarizes the acronyms used in this document.

Table 24. Acronym List

Acronym	Description
ADASTEC	ADASTEC Corp.
AWS	Amazon Web Services
BGMC	Buffalo General Medical Center
BNMC	Buffalo Niagara Medical Campus, Inc.
CAP	Comprehensive Acquisition Plan
CC	Call Center
CIP	Comprehensive Installation Plan
CISA	Cybersecurity and Infrastructure Security Agency's
CMOP	Comprehensive Maintenance and Operations Plan
CoB	City of Buffalo
COTS	Commercial-off-the-shelf
CRM	Customer Relationship Management
CTP	Complete Trip Platform
CVE	Common Vulnerabilities and Exposures
ECR	Elastic Container Registry
EKS	Elastic Kubernetes Service
ESP	Email Service Provider
ET	Eastern Time

Acronym	Description
FAQ	Frequently Asked Questions
FHWA	Federal Highway Administration
GTFS	General Transit Feed Specification
HDS	Human-Driven Shuttles
ICD	Interface Control Document
ICF	ICF International Inc.
IDE	Integrated Development Environment
IMP	Issues Management Process
INS	Indoor Navigation System
IOO	Infrastructure, owner and operator
IRB	Institutional Review Board
ITS	Intelligent Transportation System
JPO	Joint Program Office
KMS	Key Management Service
MFA	Multifactor Authentication
MOU	Memorandum of Understanding
N/A	Not applicable
NFTA	Niagara Frontier Transportation Authority
NY	New York
NYSDOT	New York State Department of Transportation
OS	Operating System
OWASP	Open Worldwide Application Security Project
PED-X	Pedestrian Crossing

Acronym	Description
PII	Personally Identifiable Information
PITR	Point-in-Time Recovery
PMD	Performance Measure Dashboard
RSD	Reservations, Scheduling and Dispatch
SaaS	Software as a Service
SAD	System Architecture Document
SDD	System Design Document
SDK	Software Development Kits
SDS	Self-Driving Shuttles
SLA	Service Level Agreement
SMS	Short Message Service
SSL	Secure Sockets Layer
SyRS	System Requirements Specification
TBD	To be determined
TIH	Transportation Information Hub
UB	University at Buffalo
UBIT	University at Buffalo / IT Department
URL	Uniform Resource Locators
USDOT	United States Department of Transportation
VIA	Visually Impaired Advancement
VoIP	Voice over Internet Protocol
WAF	Web Application Firewall

Appendix A. Service Level Agreement - INS

The following text was provided by CXApp as part of their maintenance agreement for this project.

MAINTENANCE TERMS AND CONDITIONS SCHEDULE

MAP and SDK

This Maintenance Terms and Conditions Schedule ("Maintenance Schedule") is incorporated into, and forms a part of, the Master Purchase Agreement (the "Agreement") between Company and Customer, as identified in the Agreement. Unless otherwise explicitly set forth otherwise herein, capitalized terms shall have the same meanings as set forth in the Agreement.

ARTICLE 1

Provision of Maintenance

1.1. Maintenance. Subject to Customer's payment of the applicable Fees, Company shall provide Maintenance with respect to the Products and SaaS Software, upon the terms and conditions herein, during the Maintenance Term set forth in an Order Form.

1.2. Incident Notifications. In the event of a Product or SaaS Software issue causing the Product or SaaS Software not to perform as described in the Documentation, Customer may notify Company of the issue by phone, email or ticket ("Incident Notification").

a. Company will provide Customer's designated personnel with access to our Online Service Desk for Customer's support inquiries. The Support Services provided to Customer will include the following:

- Telephone: (800) 563-8065
- Email: support@cxapp.com
- Online Service Desk: http://support.cxapp.com Track & escalate issues in a single online channel.
- Remote Support

b. The Company's Services Desk will be available for Customer's designated personnel between the hours of 6 a.m. and 5 p.m. (Pacific Standard Time), Monday through Friday, excluding Canadian statutory and United States public holidays ("Normal Service Hours"). Outside of Normal Service Hours, Customer's calls, emails and web requests will be logged electronically and Customer will receive email

confirmation thereof. Following Company's receipt of an Incident Notification, and in accordance with the Response Times set out below, Company will notify Customer that resolution activities have commenced and indicate whether Company requires any further information with respect to Customer's support request.

c. For all issues/requests received during Normal Service Hours, a Support Technician shall determine if the issue/request/question can be answered or resolved immediately, the Support Technician will:

- Notify the Customer that the issue is received and in queue – see Response Times below.

1.3. Initial Response. Upon receipt of an Incident Notification, Company will make reasonable efforts and endeavor to remotely repair reported issues with the Product or SaaS Software that prevent the Product or SaaS Software from operating in conformity with the Documentation. Company's response times and the associated resource commitment and escalation are set out in the following table:

Customer Priority (Zendesk)	Condition	First Response Time	Target Resolution / Resource Commitment
Critical (Urgent)	**Software:** Complete inability to use the software. Essential end-user components are non-functional. No convenient work-around is available. **Hardware:** Faulty device firmware (hardware failure, local software failure). Security gap identified. Beyond acceptable loss of information threshold. Non-customer network related.	2 hours	Available workaround is investigated and resolution prioritized to be addressed as soon as possible. May include: • SaaS hotfix • Software/firmware Maintenance Release or Minor Revision • Sensor replacement
Major (High)	**Software**: Major components are non- functional. Core end-user or administrative components are negatively impacted by reduced functionality or performance. The software will operate but its operation is severely restricted. Temporary work-around may or may not be available. **Hardware**: Faulty device firmware (hardware failure, local software failure). Beyond acceptable loss of information threshold. Non-customer network related.	4 hours	Where available, acceptable workaround is provided, and resolution is prioritized to be addressed in next available cycle. May include: • Next available SaaS Maintenance Release • Software/firmware Maintenance Release or Minor Revision • Sensor replacement
Minor (Low/Normal)	**Software**: Minor components are non-functional. Non-essential end-user or administrative components are impacted. The software will operate and is not materially impacted. Temporary work-around may or may not be available. **Hardware**: Faulty device firmware (hardware failure, local software failure). Within acceptable loss of information threshold. Customer network related.	24 hours	Where available, workaround will be provided, and resolution will be prioritized to be addressed in a future cycle. May include: • Upcoming SaaS Maintenance Release • Software/firmware next Maintenance Release or Minor Revision • Sensor replacement

1.4. General Updates. During the Maintenance Term, Customer is entitled to receive the following which Company generally makes available to its customers:

a. SaaS Software. With respect to SaaS Software, Customer is entitled to receive maintenance releases (also known as patches or rolling bug fixes) which Company creates on an as-required basis in its sole discretion ("Maintenance Releases"). With respect to any SaaS Hardware Deliverables included with the SaaS Software as provided in an Order Form, so long as the SaaS Hardware Deliverable has not been deemed end of life by Company, Customer is entitled to receive firmware Maintenance Releases and minor revisions, signified by a change in the decimal part of the version number (e.g., version x.1 to x.2) which may contain new functions, fixes or enhancements ("Minor Revisions").

b. Product Purchases.

• On-Premises Software. With respect to on-premises software Products that Customer purchases pursuant to an Order Form, Customer is entitled to receive Maintenance Releases and Minor Revisions.

• Sensors and Other Hardware Products. With respect to sensors or other hardware Products that Customer purchases pursuant to an Order Form, so long as the Product has not been deemed end of life by Company, Customer is entitled to receive firmware Maintenance Releases and Minor Revisions.

Customer shall not be entitled to any of the foregoing outside of the Maintenance Term.

1.5. Spare Physical Products. In the event Company determines that a physical Product, or SaaS Hardware Deliverable in connection with provision of the SaaS Software, such as a sensor, is defective and requires Maintenance, Company will make reasonable efforts and endeavor to provide Customer with a spare product for use until the issue is resolved.

1.6. Remote Maintenance. Company shall perform Maintenance remotely utilizing Customer's personnel, whom shall reasonably be made available, for assistance.

1.7. Out of Scope Maintenance. Any services, tasks, or activities not specified in this Maintenance Schedule are out of scope and may be addressed, at Company's discretion, by a Change Request or as otherwise mutually agreed by the parties. Such services, tasks, or activities include, but are not limited to, the following:

a. Installation and mounting of Products or SaaS Hardware Deliverables and network cabling to sensor network;

b. Implementation of custom Product or SaaS Software features;

c. Hardware or software upgrades to non-Company equipment or componentry;

d. Support or replacement of Products or SaaS Software having been altered, modified, mishandled, destroyed or damaged through no fault of Company's;

e. Support or replacement of Products or SaaS Software having been used by Customer or a third party other than as specified in the Documentation;

f. Support to resolve issues resulting from customer's or third-party equipment, services, or problems beyond the control of Company (which includes software defect troubleshooting); and

g. Support to resolve issues resulting from third party equipment, services, or problems beyond the control of Company (which includes software defect troubleshooting).

SAAS SOFTWARE TERMS AND CONDITIONS

SCHEDULE

This SaaS Software Terms and Conditions Schedule ("SaaS Software Schedule") is incorporated into, and forms a part of, the Master Purchase Agreement (the "Agreement") between Company and Customer, as identified in the Agreement. Unless otherwise explicitly set forth otherwise herein, capitalized terms shall have the same meanings as set forth in the Agreement.

ARTICLE 1

Provision of SaaS Software

1.1. Services. Company will provide Customer with the SaaS Software subject to the terms of the Agreement. The terms of ownership of, and other rights to, the SaaS Software, including any associated SaaS Hardware Deliverables, are set forth in Section 1.6 (SaaS Hardware Deliverables) and Article 5 (Proprietary Rights and Use) below.

1.2. License Grant. Unless otherwise limited in the applicable Order Form and subject to Customer's payment of Fees, Company grants to Customer a non-exclusive, non-transferable, royalty-free, and world-wide right to access and use the SaaS Software and any associated Documentation, only by Authorized Users (defined below), during the term set forth in the applicable Order Form in support of Customer's business and as further set out in the Order Form. Subject to the terms and conditions of this Agreement (including payment in full of all undisputed amounts by Customer), Customer's license to use the SaaS Software includes the right to use the SaaS Hardware Deliverables. All rights that Company does not expressly grant to Customer in this Section are reserved and Company does not grant any implied licenses.

1.3. Control and Location of Services. The method and means of providing the SaaS Software shall be under the exclusive control, management, and supervision of Company, and in accordance with the Documentation and as set forth in the applicable Order Form.

1.4. Authorized Users. Customer is responsible for activity by its personnel or others interacting with the SaaS Software for administration and other use on behalf of Customer ("Authorized Users"). Without limiting the foregoing, Customer shall assign, maintain, and regularly monitor accounts for Authorized Users to ensure that the SaaS Software is being used in accordance with the terms of the Agreement (which includes this Schedule) and shall immediately terminate access and use by any person who violates the terms of the Agreement. To the extent that passwords, security credentials, or authentication keys ("Passwords") are provided for use of the SaaS Software, Customer agrees to keep Passwords

strictly confidential and not provide such passwords to any unauthorized parties. Company reserves the right to terminate access to any individual in the event of any violation of the Agreement, in addition to any other remedies available to it. Customer shall promptly remove Authorized User access as appropriate when such users no longer need access. Customer shall immediately notify Company in the event that Customer or an Authorized User becomes aware of any violation of the terms of the Agreement. Any act or omission by Authorized Users is Customer's responsibility and deemed an act or omission by Customer hereunder.

1.5. Software Incorporated In SaaS Hardware Deliverables. The SaaS Hardware Deliverables may include certain software or middleware incorporated into the SaaS Hardware Deliverables. Such software or middleware is subject to the terms of this Agreement and as part of the SaaS Software is subject to any additional terms of use provided by Company electronically, or otherwise, in connection with their download or installation. Such software or middleware shall be used solely by Authorized Users.

1.6. SaaS Hardware Deliverables. With respect to any hardware or other physical equipment or items made available to Customer in connection with the SaaS Software ("SaaS Hardware Deliverables"), unless otherwise expressly sold to Customer as a Product pursuant to an Order Form, Company retains all right, title and interest in the SaaS Hardware Deliverables, including all units and spare parts thereof. Company retains all such rights notwithstanding installation of the SaaS Hardware Deliverables at the Customer's location. Customer shall not pledge, mortgage, subject to lien or otherwise encumber the SaaS Hardware Deliverables or take any other action contrary to Company's exclusive, unencumbered ownership thereof. Customer shall return all SaaS Hardware Deliverables to Company upon Company's request and in any event upon termination of the Agreement or expiry of the SaaS Software Term, and shall be responsible to Company for all loss or damage to the SaaS Hardware Deliverables, except where directly caused by Company.

1.7. Customer Platform. Customer shall be responsible for procuring and maintaining the platform elements, including equipment, hardware, and computing environment, as may be designated by Company from time to time in an Order Form or otherwise.

1.8. Replacement/Alteration of Equipment. Company may, at its own cost, in instances necessitated for reasons critical to the performance of Company's network or important to quality or consistency of its provisioning of the SaaS Software, in Company's absolute discretion and without notice to the Customer, make changes to or replace the SaaS Hardware Deliverables, provided that the quality is not materially adversely affected. In other instances, where in Company's opinion the SaaS Hardware Deliverables should be changed or replaced, Company agrees to consult with Customer and Company and Customer, acting reasonably, will mutually agree on a schedule for the replacement of the applicable SaaS Hardware Deliverables.

1.9. Access.

a. Company Access. Company may, upon reasonable notice under the circumstances, make such inspections, tests, installations and adjustments as it deems necessary for the operation of the SaaS Software or Company's network, SaaS Hardware Deliverables or connecting facilities. Customer agrees to make available to Company, without charge, such facilities and equipment (including providing access to Customer premises or facilitating such access where Customer is a tenant) as are reasonably necessary under the circumstances.

b. Customer Access. The Customer shall not, without Company's prior written consent and then subject to such conditions as Company may require, make any alteration, addition or repair to the SaaS Hardware Deliverables or any other provisions of the SaaS Software.

ARTICLE 2

Term and Termination

2.1. Term of Services. The initial term of each SaaS Software purchase set forth in an Order Form begins on the date set forth within the Order Form and will continue for the period of time set forth within the Order Form, subject to earlier termination in accordance with this Section 2.1 (Term of Services) or Section 3.2 of the Agreement (Termination for Cause) (the "Initial SaaS Service Term"). FOLLOWING THE INITIAL SAAS SOFTWARE TERM, THE SAAS SOFTWARE TERM (AS DEFINED BELOW) SHALL AUTOMATICALLY RENEW FOR SUCCESSIVE PERIODS EQUAL TO THE INITIAL SAAS SOFTWARE TERM (EACH, A "RENEWAL SAAS SOFTWARE TERM"), UNLESS EITHER PARTY TERMINATES SUCH SAAS SOFTWARE PURCHASE BY PROVIDING WRITTEN NOTICE OF SUCH INTENTION AT LEAST NINETY (90) DAYS PRIOR TO THE END OF THE INITIAL SAAS SOFTWARE TERM OR ANY RENEWAL SAAS SOFTWARE TERM, AS THE CASE MAY BE.

The Initial SaaS Software Term and any Renewal SaaS Software Term(s) shall be collectively referred to as the "SaaS Software Term"

2.2. Termination by Company. In addition to early termination provided for in Section 3.2 (Termination for Cause) or Section 3.3 (Termination for Convenience) of the Agreement, without incurring liability, Company may terminate, restrict, or suspend the SaaS Software, upon prior written notice (and failure to cure, if applicable) set out in parentheses after each ground for termination, if the Customer:

a. becomes the subject of a voluntary or involuntary petition in bankruptcy or any proceeding relating to insolvency, receivership, liquidation or composition for the benefit of creditors that is not dismissed within sixty (60) days (no notice required); or

b. where any law, order, or commercially unreasonable impediment prohibits Company from furnishing such Services (the lesser of (30) days' notice or as long as compliance allows).

2.3. Termination by Customer. If Customer terminates the SaaS Software for any reason other than as permitted under in Section 3.2 of the Agreement (Termination for Cause), Customer shall pay to Company, as liquidated damages and not as a penalty, and in addition to any validly incurred charges to the date of termination, an amount equal to the sum of all remaining Fees for the SaaS Software Term set forth in the applicable Order Form. Customer acknowledges and agrees that the foregoing liquidated damages provision is reasonable in light of the anticipated or actual harm caused by Customer's termination of the Agreement, the difficulties of proof of loss and the inconvenience or non-feasibility of otherwise obtaining an adequate remedy.

ARTICLE 3

Warranties

3.1. Limited Warranty. Company warrants that the SaaS Software shall function substantially as set forth in the Documentation during the SaaS Software Term.

3.2. Limited Remedy. Customer's sole remedy and Company's sole liability under the limited warranty of Section 3.1 (Limited Warranty) shall be for Customer to receive and Company to provide Maintenance in accordance with the Maintenance Schedule, subject to the terms of this Agreement including payment of the Fees by Customer.

3.3. Disclaimer of Warranties. THE FOREGOING LIMITED WARRANTY IS THE EXCLUSIVE WARRANTY WITH RESPECT TO THE SERVICES, AND, EXCEPT TO THE EXTENT PROHIBITED BY APPLICABLE LAW, ANY OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, NONINFRINGEMENT, OR ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE ARE EXPRESSLY DISCLAIMED BY COMPANY AND WAIVED BY CUSTOMER.

3.4. Exclusions. Company's obligations under this Article 3 do not extend to any relocation, maintenance, repair, alteration, modification, or adjustment which becomes necessary due to, resulting from or in any way related to, damage, negligence, or misuse on the part of Customer.

ARTICLE 4

Indemnification

4.1. Company Indemnity. Company shall defend any action brought against Customer to the extent that it is based upon a claim that the SaaS Software, as provided by Company to Customer under the Agreement and used as permitted within the scope of the Agreement, infringe any copyright or patent of a third party under the laws of the United States (an "Indemnity Claim"), and shall pay any costs, damages and reasonable attorneys' fees attributable to such claim that are awarded against Customer, provided that Customer:

(a) notifies Company in writing within thirty (30) days of receipt of the Indemnity Claim; (b) grants Company sole control of the defense and settlement of the Indemnity Claim; and (c) provides Company, at Company's expense, with all reasonable assistance, information and authority required for the defense and settlement of the Indemnity Claim.

4.2. Infringement; Injunctions. If Customer's use of the SaaS Software hereunder is, or in Company's opinion is likely to be, enjoined as an infringement of any third party copyright or patent under the laws of the United States, Customer's sole and exclusive remedy, and Company's entire liability, shall be, at Company's sole option and expense, either: (a) to procure for Customer the right to continue to use the SaaS Software under the terms of the Agreement; (b) replace or modify the SaaS Software so that it is non- infringing; or, if neither of the foregoing options is commercially reasonable, (c) terminate the Agreement in whole or in part, after which Customer shall be under no obligation to pay Fees under the Agreement for usage after the termination date.

4.3. Exclusions. Notwithstanding the terms of Section 4.1 (Company Indemnity), Company shall have no liability for any claim of any kind to the extent it results from: (a) directions, designs, plans or specifications furnished by or on behalf of Customer; (b) unauthorized use, or use of the SaaS Software in violation of this Agreement; (c) any data uploaded or provided by Customer or an end user; (d) any activities of Customer or end user through the use of the SaaS Software; (e) modification of the SaaS Software made other than by Company; (f) the combination, operation or use by Customer of the SaaS Software with equipment, devices or software not supplied by Company; (g) failure of Customer to use

updated or modified SaaS Software provided by Company, including those provided to avoid infringement; or (h) Customer's use of the SaaS Software after termination of this Agreement.

4.4. Sole Remedy. THE FOREGOING PROVISIONS OF THIS ARTICLE 4 (INDEMNIFICATION) SET FORTH COMPANY'S SOLE AND EXCLUSIVE OBLIGATIONS, AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES, WITH RESPECT TO INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS OF ANY KIND.

4.5. Customer Indemnity. Customer agrees to indemnify and hold Company and its directors, employees, agents, and distributors harmless from any cost, liability or loss relating to any of the items in Section 4.3 (Exclusions) or Customer's obligations under Article 5 (Proprietary Rights and Use).

ARTICLE 5

Proprietary Rights and Use

5.1. Company Ownership. Except for the rights granted to Customer in Section 1.2, and Company's rights to Customer Data (defined below), as between the parties, Company retains all right, title and interest, including all intellectual property rights, in and to the SaaS Software and SaaS Hardware Deliverables and all aggregated and de-identified information that Company's systems or applications automatically collect in relation to the SaaS Software and/or its use and/or performance (including, without limitation, de-identified data that does not, and cannot reasonably be used to, identify Customer or any individual) ("Diagnostic Data").

5.2. Customer Ownership. As between the parties, Customer owns all data, information and other materials submitted to the SaaS Software (which, for clarity, excludes Diagnostic Data) (collectively, "Customer Data"). Customer hereby grants to Company a non-exclusive and non-transferable license to use and host the Customer Data, solely to provide the SaaS Software. Company represents and warrants that: (i) it either owns the Customer Data or is otherwise permitted to grant the license set forth in this Section; (ii) the posting and use of the Customer Data on or through the SaaS Software does not violate the privacy rights, publicity rights, copyrights, contract rights, intellectual property rights, or any other rights of any person. Company is not responsible for the content of any Customer Data or the way Customer or its Authorized Users choose to use the SaaS Software to store or process any Customer Data.

5.3 Customer Obligations. Customer represents and warrants and covenants that: (i) Customer will comply with all applicable privacy and data protection laws and regulations applicable to its business with respect to any Customer Data uploaded to, submitted to, stored on, or processed by the SaaS Software; and (ii) Customer will obtain any required consent prior to commencement of Customer's use of the SaaS Software (including, without limitation any consent needed for personally identifiable information) to transfer Customer Data to Company and to permit Company to store, process, retrieve, and disclose such Customer Data as contemplated by this Agreement; and (iii) Customer shall be responsible for the Customer's and Authorized Users' use of the SaaS Software and Content. The Customer acknowledges that Company does not own or have any control over the Content accessible or that may be available to or by the Customer or its Authorized Users through the use of the SaaS Software. The Customer's and Authorized Users' use of the SaaS Software and Content shall, at all times, comply with the Agreement (including this SaaS Software Schedule) and the

Customer shall not use nor permit usage of any SaaS Software for any improper use. Customer assumes all risk arising from any use of the SaaS Software by Customer or Authorized Users that is not compliant with applicable laws. Company is not required to preserve and provide the Customer Data to Customer unless expressly provided in writing regarding terms and costs for such service.

5.3. Data Protection Requirements. The parties shall comply with the terms found in Exhibit A to this SaaS Software Schedule.

5.4. Resale. Unless otherwise agreed upon, Customer shall not resell the SaaS Software, including any SaaS Hardware Deliverables (or otherwise make the SaaS Software or SaaS Hardware Deliverables available to third parties for value). If Customer has resold SaaS Software or SaaS Hardware Deliverables without the consent of Company, in addition to any other remedies available to Company, Company shall have the right to (a) suspend the SaaS Software or invoke return of the SaaS Hardware Deliverables, as applicable and/or (b) immediately terminate the Agreement or the applicable SaaS Software.

5.5. Other Suspension or Termination. Unless otherwise required by law or regulatory authority, Company may, acting reasonably and without incurring liability: (a) cancel a request for SaaS Software; (b) suspend or terminate the SaaS Software and/or the Agreement; or (c) temporarily block SaaS Software to Customer premises if Company deems such action necessary to prevent improper use, to protect against fraud or the commission of suspected illegal activities, to otherwise protect its personnel, agents, facilities or services, or to prevent Customer's use of the SaaS Software from interfering with Company's ability to provide services to the Customer or others. Company will use reasonable efforts to provide notice to Customer before taking action under this Section.

EXHIBIT A

GLOBAL DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") supplements the Agreement between Company and Customer (jointly "the Parties"), in relation to your use of the SaaS Software to Process Personal Data. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the Parties including the Agreement and this DPA, the terms of this DPA will control.

1 DEFINITIONS.

Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below.

1.1 "Aggregated Information" means information that relates to a group or category of natural persons, from which individual identifies have been removed, that is not linked or reasonably linkable to any consumer, household, or device.

1.2 "Agreement" means any agreement between Company and a specific customer under which SaaS Software is provided by Company to that customer. Such an agreement may have various titles, including but not limited to "Order Form," "Sales Order," or "Terms of Service."

1.3 "CCPA" means the California Consumer Privacy Act of 2018, as amended.

1.4 “Controller” means the party that determines the purposes and means of the Processing of Personal Data, and includes a “business” as defined in the CCPA.

1.5 “Data Protection Laws” means all laws and regulations, including laws and binding regulations of the European Union, the European Economic Area (“EEA”) and their member states, Switzerland and the United Kingdom, and any amending or replacement legislation from time to time, applicable to the Processing of Personal Data under the Agreement.

1.6 “Deidentified Information” means information that cannot reasonably identify, relate to, be capable of being associated with, or be linked, directly or indirectly, to a particular individual.

1.7 “GDPR” means the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC.

1.8 “Personal Data” means any information relating to an identifiable individual (as defined by the GDPR, and “personal information” as defined by the CCPA), that is Processed by Company on Customer’s behalf. For the avoidance of doubt “Content”, as defined in the Agreement, may comprise Personal Data.

1.9 “Permitted Purpose” means the use of the Personal Data to the extent necessary for provision of the SaaS Software by Company to the Customer.

1.10 “Processor” means the party which Processes Personal Data on behalf of the Controller, and includes a “service provider” as defined in the CCPA.

1.11 “Regulator” means any entity which has jurisdiction to enforce Customer’s and the Company’s compliance with the Data Protection Laws.

1.12 “Security Incident” means any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of Personal Data.

1.13 “SaaS Software” has the same meaning as in the Agreement.

1.14 “Standard Contractual Clauses” means the agreement, available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087 (as amended, superseded or replaced from time to time), pursuant to the European Commission decision (C(2010)593) of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC.

1.15 “Sub-processor” means any entity engaged by Company to Process Personal Data in connection with the Services.

1.16 Terms such as “Business Purpose”, “Commercial Purpose”, “Consumer”, “Data Subject”, “Processing” (and “Process”), “Sale”, and “Sell” shall have the meaning ascribed to them in the Data Protection Laws.

1.17 “Third-Party Services” means connections and/or links to third party websites and/or services not included in the core Services offerings identified in the Agreement, including, without limitation, via application programming interfaces.

2. DATA PROCESSING

2.1 Details of Processing.

2.2 Roles of the Parties. The Parties acknowledge and agree that Company will Process the Personal Data in the capacity of a Processor and that Customer will be the Controller of the Personal Data. Customer understands that to the extent Third-Party Services are accessed, Customer serves as the Controller and the Third-Party Services are Processors, and the Third-Party Services are not Sub-processors of Company.

2.3 Customer Instructions. The Parties agree this DPA and the Agreement constitute Customer’s documented instructions regarding Company’s processing of Personal Data. Company will process Personal Data only in accordance with these documented instructions. Company may convert Customer Data into Aggregated Information or Deidentified Information, which, notwithstanding anything to the contrary, Company may fully exploit.

2.4 Compliance with Laws. Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA. Company is not responsible for determining the requirements of laws applicable to Customer’s business or that Company’s provision of the Services meet the requirements of such laws.

3. CUSTOMER’S OBLIGATIONS

3.1 Instructions. Customer shall warrant that the instructions it provides to Company pursuant to this DPA comply with the Data Protection Laws.

3.2 Data Subject and Regulator Requests. Subject to the applicable Data Protection Law, the Customer shall be responsible for communications and leading any efforts to comply with all requests made by Data Subjects under the Data Protection Laws, and all communications from Supervisory Authorities that relate to Personal Data, in accordance with Data Protection Laws. To the extent such requests or communications require Company’s assistance, the Customer shall notify Company of the Data Subject or Regulator request.

3.3 Notice, Consent and Other Authorizations. Customer is responsible for providing the necessary notice to the Data Subjects under the Data Protection Laws. Customer is responsible for obtaining, and demonstrating evidence that it has obtained, all necessary consents, authorizations and required permissions under the Data Protection Laws in a valid manner for Company to perform the Services.

3.4 Signage. Where Content comprises Personal Data to which Applicable Data Protection Law applies, and where Applicable Data Protection law imposes data subject notification requirements (including but not limited to the GDPR and the CCPA), Customer agrees to place clear signage around the premises in which the SaaS Software are to be provided, the purpose of which is to advise data subjects that the form of monitoring identified in the applicable Order Form is taking place. The signage must also link to a compliant privacy statement or policy.

4. COMPANY'S OBLIGATIONS

4.1 Scope of Processing.

4.1.1 Company will Process Personal Data on documented instructions from the Customer, and in such manner as is necessary for the provision of the SaaS Software except as required to comply with a legal obligation to which Company is subject. If Company believes any documented instruction or additional processing instruction from Customer violates the GDPR, Company will inform Customer without undue delay and may suspend the performance of the SaaS Software until Customer has modified or confirmed the lawfulness of the additional processing instruction in writing. Customer acknowledges and agrees that Company is not responsible for performing legal research or for providing legal advice to Customer.

4.1.2 In relation to the CCPA and similarly situated Data Protection Laws, the parties acknowledge and agree that Company is a service provider and receives Company Data pursuant to the Business Purposes of providing the SaaS Software to Company in accordance with the Agreement. For the avoidance of doubt, Company shall not: (a) Sell Personal Data; (b) collect, retain, use, or disclose Personal Data for any purpose other than for the specific purpose of performing the Agreement; (c) collect, retain, use, or disclose Personal Data for a Commercial Purpose other than providing the SaaS Software according to the Agreement; or (d) collect, retain, use, or disclose Personal Data outside of the direct business relationship between Company and Customer. Company agrees that it does not and will not receive any Personal Data as consideration for any services or other items that Company provides to Customer, and shall not have, derive, or exercise any rights or benefits regarding Personal Data. Company certifies that it understands the restrictions in this Section and will comply with them in accordance with the requirements of applicable Data Protection Laws.

4.2 Cooperation. If Company receives a request from any Data Subject made under Data Protection relating to Personal Data, Company will provide a copy of that request to the Customer within two (2) business days of receipt. Company will provide reasonable assistance to the Customer in responding to the request. Company will assist Customer in addressing any communications and abiding by any advice or orders from the Regulator relating to the Personal Data. Taking into account the nature of the Processing and the information available, Company will provide reasonable assistance to Customer in complying with its obligations under GDPR to complete data protection impact assessments.

4.3 Retention. Company will retain Personal Data only for as long as the Customer deems it necessary for the Permitted Purpose, or as required by applicable laws. At the termination of this DPA, or upon Customer's written request, Company will either destroy or return the Personal Data to the Customer, unless legal obligations require storage of the Personal Data.

4.4 Disclosure to Third Parties and Confidentiality. Company will not disclose the Personal Data to third parties except as permitted by this DPA or the Agreement, unless Company is required to disclose the Personal Data by applicable laws, in which case Company shall (to the extent permitted by law) notify the Customer in writing and liaise with the Customer before complying with such disclosure request. Company treats all Personal Data as strictly confidential and requires all employees, agents, and Sub-processors engaged in Processing the Personal Data to commit themselves to confidentiality, and not Process the Personal Data for any other purposes, except on instructions from Customer.

4.5 Security. Company has implemented and will maintain reasonable and appropriate administrative, physical, technical and organizational safeguards for the security (including protection against accidental or unlawful loss, destruction, alteration, damage, unauthorized disclosure of, or access to, Personal Data

transmitted, stored or otherwise Processed), confidentiality and integrity of Personal Data. In assessing the appropriate level of security, Company shall take into account the risks that are presented by Processing, in particular from accidental, unauthorized, or unlawful destruction, loss, alteration, damage, disclosure of, or access to Personal Data transmitted or stored.

5. CONTRACTING WITH SUB-PROCESSORS

5.1 General Consent. Customer agrees that Company may engage third-party Sub-processors in connection with the provision of the SaaS Software, subject to compliance with the requirements below. As a condition to permitting a Sub-processor to Process Personal Data, Company will enter into a

written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2 No Current Sub-processors. The Company does not currently utilize Sub-processors for the provision of the SaaS Software.

5.3 New Sub-Processors. Company will provide Customer with notice ("New Sub-processor Notice") of the addition of any new Sub-processor at any time during the term of the Agreement. If Customer has a reasonable basis to object to Company's use of a new Sub-processor, Customer will notify Company promptly in writing within 15 days after receipt of a New Sub-processor Notice. Company will use reasonable efforts to make available to Customer a change in the affected SaaS Software or recommend a commercially reasonable change to Customer's configuration or use of the affected SaaS Software to avoid processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Company is unable to make available such change within a reasonable period of time, which will not exceed 30 days, Customer may terminate the portion of any Agreement relating to the Services that cannot be reasonably provided without the objected-to new Sub-processor by providing written notice to Company.

5.5 Responsibility. As between Company and Customer, Company will remain responsible for its compliance with the obligations of this DPA and for any acts and omissions of its Sub-processors that cause Company to breach any of Company's obligations under this DPA.

6. SECURITY INCIDENT MANAGEMENT. Company shall, to the extent permitted by law, notify Customer without undue delay, but no later than 48 hours after becoming aware of any Security Incident. Company's notification of a Security Incident to the Customer to the extent known should include: (a) the nature of the incident; (b) the date and time upon which the incident took place and was discovered; (c) the number of data subjects affected by the incident; (d) the categories of Personal Data involved; (e) the measures – such as encryption, or other technical or organizational measures – that were taken to address the incident, including measures to mitigate the possible adverse effects; (f) whether such proposed measures would result in a disproportionate effort given the nature of the incident; (g) the name and contact details of the data protection officer or other contact; and (h) a description of the likely consequences of the incident. The parties will cooperate regarding notification required under the Data Protection Laws to data subjects and any public authority.

7. TRANSFERS OUTSIDE THE EUROPEAN ECONOMIC AREA

7.1 Company shall not transfer, or participate in any transfer or onward transfer of Personal Data that is collected from a Data Subject located in the European Economic Area (EEA), the United Kingdom or Switzerland ("EEA Personal Data") to a jurisdiction that has not been recognized as providing adequate data protection by the EU, without putting in place an appropriate transfer agreement or other mechanism that complies with the GDPR.

7.2 The parties agree that Standard Contractual Clauses will apply to EEA Personal Data that is transferred from Customer to Company, either directly from the EEA or via onward transfer, to any country not recognized by the European Commission as providing as adequate level of protection for personal data (as described by the GDPR).

8. AUDITS

8.1 Audits. Customer, at its sole expense, may audit Company's compliance with this DPA up to once per year, unless requested by a Regulator or in the event of a Security Incident. Such audit will be conducted by an independent third party ("Auditor") reasonably acceptable to Company. Before the commencement of any such on-site audit, Customer must submit a detailed proposed audit plan to Company at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration and state date of the audit. Company will review the proposed audit plan and provide Customer with any concerns or questions. Company will work cooperatively with Customer to agree on a final audit plan. The results of the inspection and all information reviewed during such inspection will be deemed Company's confidential information and shall be protected by Auditor in accordance with the confidentiality provisions noted above. Notwithstanding any other terms, the Auditor may only disclose to the Customer specific violations of the DPA, if any, and the basis for such findings, and shall not disclose to Customer any of the records or information reviewed during the inspection.

9. MISCELLANEOUS

9.1 Obligations Post-termination. Termination or expiration of this DPA shall not discharge the parties from their obligations meant to survive the termination or expiration of this DPA.

9.2 Severability. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. The parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and shall incorporate such substitute provision into this DPA.

Appendix B. Service Level Agreement - Redyref

The following is the “Gold Level” Service Level Agreement currently in place with Redyref

REDYREF MASTER SERVICES AGREEMENT

This **MASTER SERVICES AGREEMENT** (this “Agreement”) is made and entered into by and between EVS Interactive, Inc. (dba REDYREF Interactive Kiosks and Livewire Digital), a New Jersey Corporation ("**REDYREF**”) with offices at 100 Riverdale Road, Riverdale, NJ 07457 and the customer whose name appears on the signature block of this Agreement ("Customer"). This Agreement shall apply to each and every “Statement of Work” executed by REDYREF and Customer. Each Statement of Work hereunder is governed by this Agreement.

1.INTRODUCTION

1.1 REDYREF owns various hardware designs and computer-based applications commonly known as the Engage IoT® Content Management Software Suite (the “Technology”).

1.2 Customer desires to retain REDYREF, to provide services as an independent contractor, in accordance with the following terms and conditions and REDYREF desires to provide services in accordance with the following terms and conditions.

1.3 Customer desires to obtain a license from REDYREF to use the Technology which allows the Customer to provide information through their remotely managed devices (kiosks, digital signs, and mobile devices) by accessing the Technology remotely.

1.4 REDYREF is willing to grant to Customer license to use the Technology and to provide certain services with respect to the Technology, on the terms and conditions set forth herein.

1.5 The kiosk design remains the exclusive property of REDYREF or its manufacturing partners. All rights reserved. Reproduction rights in any form go to REDYREF.

1.6 When Customer is acquiring hardware only, any term or provision herein relating to software shall be inapplicable.

2.DEFINITIONS

2.1 **"Licensed Software"** shall mean the REDYREF proprietary computer software platform commonly known as the Engage IoT® Content Management Software Suite, and other proprietary application software that REDYREF has acquired the rights to modify and distribute, and all modules thereof, with functional and operational content commercially available as of the effective date of this Agreement. REDYREF Standard Software includes, without limitation, Engage IoT Server Software and Engage IoT Client Software.

2.2 **"Custom Software"** means the application programs being written exclusively for the Customer and described in Functional Specifications or other documents and includes the programs or modules written to adapt the Standard Software to the Customer's requirements, Hardware, or other components of the Customer's computer system, to the extent that such programs and modules are not permanently embedded in the Standard Software and are easily separable from the Standard Software.

2.3 **"Documentation"** shall mean user guides and other materials made available by REDYREF to Customer in written or electronic form.

2.4 **"Live Operation"** shall mean the operation of the Software on the Hardware without significant error or down time, in processing real financial transactions impacting real accounts.

2.5 **"Standard Enhancements"** shall mean those improvements, additions and revisions to the Licensed Software and/or Documentation that are part of the scheduled software development or maintenance plan of REDYREF and are implemented for REDYREF's licenses and are included in the annual maintenance fees.

2.6 **"Optional Enhancements"** shall mean any improvements, additions and revisions to the Licensed Software and/or Documentation that are developed by REDYREF and are offered to Customer for an additional fee.

2.7 **"REDYREF Software License Fees"** shall mean the applicable license fees charged by REDYREF for licensing and annual maintenance of the software per unit and described and identified in an SOW/PROPOSAL.

2.8 **"REDYREF Professional Service Rates"** shall mean the applicable rates charged by REDYREF for specific professional services in effect at the time such services are performed and described and identified in an SOW/PROPOSAL.

2.9 "**Functional Specifications**" means formal documents prepared by REDYREF agreed to in writing by Customer, if applicable, or as otherwise set forth in the applicable Documentation provided by, or to, Customer which set forth the parameters, specification, configuration, scope, and characteristics of a system of computer hardware or software.

2.10 "**Statement of Work**" or "**SOW/PROPOSAL**" means REDYREF's standard form of statement of work or proposal accepted by REDYREF and Customer, or a separate schedule or addendum that specifies Products and Services ordered by Customer and executed by the Parties. An SOW/PROPOSAL may be captioned "Proposal", "Work Order", "Purchase Order" or similar.

2.11 “**Transaction Fee**” shall mean the applicable fees charged by REDYREF for processing a sale, purchase, or some other action recorded in REDYREF’s hosted services database. The transaction fee is typically a percentage of dollar value of the transaction, but it may also consist of a flat rate per transaction or a combination of both.

3. LICENSED RIGHTS

3.1 Licensed Software. REDYREF hereby grants to Customer, and Customer hereby accepts from REDYREF, during the term of this Agreement and subject to compliance by Customer with the terms and conditions hereof, a nonexclusive, nontransferable, nonassignable license to access and use the Licensed Software solely for Customer’s internal business purposes.

3.2 Restrictions on Licensed Rights. Customer acknowledges that the components of the Licensed Software are subject to copyrights and other intellectual property rights owned by REDYREF. Customer is prohibited from copying, duplicating, or permitting anyone else to copy or duplicate the Licensed Software or any portion thereof. Customer is further prohibited from (a) using the Licensed Software to process any data other than Customer's own data and (b) modifying, adapting, or creating derivative works based on the Licensed Software.

3.3 No Ownership. Nothing contained in this agreement shall act or be construed to be a sale, assignment, or transfer of REDYREF’s IP to Customer, any such sale, assignment or transfer being hereby specifically denied and disclaimed by REDYREF and Customer. Any documentation or information which REDYREF may provide to Customer regarding the Product (or the maintenance or repair thereof) and including but not limited to REDYREF’s IP, shall be deemed to be and remain REDYREF’s Confidential Documents and Information and may not be used by Customer (or provided by Customer to any third parties, or used by any third parties) except for the limited and exclusive purpose of repairing or maintaining the Product.

4. SET UP, CONDITIONS, CONFIGURATION, WARRANTY, MAINTENANCE, SUPPORT AND TRAINING

4.1 Set Up. REDYREF shall provide assistance to Customer in connection with the implementation of the Licensed Software at a per-hour fee or pre-defined fee set forth in an SOW/PROPOSAL.

4.2 Changed Conditions. If not listed in the Functional Specifications, and project conditions have been discovered which were not known to REDYREF at the time the Agreement was made (provided REDYREF has performed such due diligence as time permits, on the project conditions prior to REDYREF’s execution of the Agreement), and if such changed conditions require the pricing, payment schedule or scope of work to be modified, REDYREF shall provide written Notice to Customer within ten (10) days of the event giving rise to such opinion, stating the basis for REDYREF’s opinion, and requesting that Customer negotiate with REDYREF towards an amendment to the Agreement(s) as necessary. If negotiations relating changed conditions do not result in an amendment acceptable to both parties, and any changes in the compensation not agreed upon by the parties shall be determined by arbitration as provided below, or the parties may terminate this Agreement. The above notwithstanding, Customer shall remain liable for all charges incurred prior to termination of this Agreement.

4.3 Delays. Any one or more suspensions caused by Customer may have a direct impact on the originally defined project schedule and may result in one-to-one day (or more) delay of REDYREF deliverables. Unless the invoiced work is disputed by Customer, scheduled payment of invoices from REDYREF,

however, will continue per the original payment milestone schedule set forth in SOW/PROPOSAL. Any customer delay of ten (10) or more consecutive days may cause the project to be placed on hold, and additional costs may be incurred if REDYREF is unable to proceed with the work effort due to customer's delays. These costs shall be billed to Customer at REDYREF's standard time and material charges set forth in an SOW/PROPOSAL.

Delivery/shipment dates are good faith estimates, and REDYREF SHALL, in good faith, endeavor to ship the work by the estimated date. REDYREF SHALL NOT BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, SECONDARY, OR INCIDENTAL DAMAGES, HOWEVER ARISEN, DUE TO LATE DELIVERY.

4.4 Configuration. REDYREF shall perform reasonable and ordinary ongoing configuration of the parameters of the Licensed Software to Customer's requirements in a manner that does not require custom modification of the Licensed Software at a per hour fee or pre-defined fee set forth an SOW/PROPOSAL but only after giving Customer prior notice of REDYREF's intent to perform configuration that generates fees for Customer.

4.5 Operational Support. A member of the REDYREF client services support staff will be available during the hours of 8:30 a.m. to 5:00 p.m. Eastern Time, Monday through Friday, to answer questions by telephone and email regarding the Product. Any work required by REDYREF that is not supported under the agreed upon service level (please see separate "Managed Service Agreement" if applicable), Customer shall be charged for operational support services provided at the applicable REDYREF standard service rates or as set forth in an SOW/PROPOSAL.

4.6 Database Maintenance. REDYREF has the sole right and responsibility to maintain and update the logical and physical organization and structure of the databases and associated files within the Licensed Software. In connection with such maintenance and update, Customer shall provide to REDYREF any testing assistance that REDYREF may reasonably request, but REDYREF shall provide Customer notice prior to commencing Database Maintenance.

4.7 Training. REDYREF shall provide Customer with initial standard training on the operation of the Licensed Software and any Custom Software. To the extent that such training is provided by REDYREF at Customer's site the fees for providing such training shall be the Customer's and be billed to the Customer at REDYREF's standard time and material charges or as set forth in an SOW/PROPOSAL.

4.8 Custom Software Warranty; Third Party Warranties. REDYREF warrants that for the thirty (30) day period commencing with the date of Acceptance by Customer of the Custom software (the "Warranty Period"), the Custom software will conform, as to all material operational features as documented in the Functional Design Documentation. If any modifications, corrections and/or upgrades are made by Customer to the Custom software or third-party software affecting the Custom Software during the Warranty Period, the warranty given herein shall immediately be terminated with respect to that portion of the Custom Software that is modified or affected by the modification, correction and/or upgrade. Corrections in the Custom Software for difficulties or defects traceable to modifications made by Customer shall be billed to Customer at REDYREF's standard time and material charges or as set forth in an SOW/PROPOSAL. REDYREF makes no representations, and specifically disclaims any warranties, with respect to equipment, software, services, or other deliverables developed or provided by third parties.

4.9 Support of Custom Software. Upon request of Customer, REDYREF shall provide maintenance and support for the Custom Software after the expiration of the Warranty Period specified in 4.8. Unless otherwise specified in this Agreement or within a separate Annual Custom Support Agreement, the fees for providing maintenance on Custom Software will be billed at the standard time and material rate or as set for in an SOW/PROPOSAL.

4.10 REDYREF Licensed Software. Customer acknowledges that the Licensed Software resides on each device/unit utilizing REDYREF Technology and will be billed at the standard published prices or as set for in an SOW/PROPOSAL.

4.11 REDYREF Hosted Services. If Customer is utilizing REDYREF's hosted services, the following shall apply:

4.11.1 REDYREF Servers. The Licensed Server Software shall be installed and maintained from REDYREF's servers powered by Microsoft Azure (or equivalent hosting provider). Web access to administration and reporting services and remote monitoring of each system is included.

4.11.2 Data Maintenance. REDYREF shall maintain daily back-up of any data stored in the REDYREF computing environment. REDYREF shall provide all other data maintenance services, including without limitation loading Customer data on the Servers and converting Customer databases. Customer acknowledges that REDYREF shall have no obligation or responsibility to Customer for loss, destruction or damage to any Customer data stored in the REDYREF computing environment that results from Customer's conduct.

4.11.3 Standard Enhancements. REDYREF reserves the right, as reasonably necessary or convenient for REDYREF's own purposes or to improve the quality of the Licensed Software, to change access procedures, types of equipment utilized in the REDYREF computing environment, system interfaces, operating and other system and network software, utilities, and database software, and to implement Standard Enhancements to the Licensed Software. Whenever practicable, REDYREF shall give Customer advance notice of the scheduled implementation of any Standard Enhancement. REDYREF agrees to make every reasonable effort to implement Standard Enhancements during off hours and without interrupting Customer's regular business operations.

4.11.4 Access Interruptions. Customer acknowledges and agrees that for REDYREF to perform the maintenance services set forth herein, REDYREF may be required from time to time to interrupt Customer's ability to access the Licensed Software and/or the REDYREF computing environment. Insofar as practicable, REDYREF shall confine such interruptions to scheduled interruptions and give Customer advance notice of a scheduled interruption.

4.11.5 Error Investigation: While under a support agreement, if the Licensed or Custom software becomes inaccessible or its operation deviates materially from the SOW/PROPOSAL, REDYREF will use commercially reasonable efforts to remotely diagnose the cause of the inaccessibility or deviation. Upon completion of the diagnosis, REDYREF shall advise Customer of the cause of the inaccessibility or deviation. If it is determined by REDYREF inaccessibility or deviation is the Licensed or Custom Software, REDYREF will restore access to the Software at no charge. If any inaccessibility or deviation is determined not to be attributed to the Licensed Software, REDYREF will invoice the Licensee for the cost of the diagnosis in accordance with the applicable REDYREF Service Rates and provide an estimate to assist with repair of the issue, if applicable.

4.12 Limited Warranty: REDYREF-manufactured products come with a limited 1-year warranty. This limited warranty covers defects in materials and workmanship in your REDYREF products. The warranty period offered by REDYREF begins at date of shipment but does not include coverage of damage that may occur in transit if the Customer signs for the damaged shipment at delivery. This limited warranty covers:

- Unlimited remote troubleshooting of hardware defects;
- Repair and replacement of malfunctioning equipment due to manufacturer defects;
- Repair/replacement based on Customer shipment of faulty equipment to REDYREF and REDYREF return of repaired/replaced equipment to Customer (shipment via ground service);
- Billable onsite support, if necessary.

This limited warranty does not cover:

- Software not provided by REDYREF, including without limitation, the operating system;
- Non REDYREF-provided products and accessories;
- Problems that result, directly or indirectly, from:
    - o Defects, failures, damages or performance limitations caused in whole or in part by (A) power failures, surges, failures in third-party communication networks, fires, floods, snow, ice, lightning, excessive heat or cold, highly corrosive environments, accidents, vandalism, actions of third parties, or other events outside of REDYREF's control, or (B) the customer's abuse, mishandling, misuse, computer viruses, negligence, improper storage, or unauthorized attempts to repair or alter the equipment or component in any way
    - o Improper ventilation by Customer
    - o Servicing not authorized by REDYREF
    - o Usage that is not in accordance with product instructions
    - o Failure to follow the product instructions or failure to perform preventive maintenance
    - o Using accessories, parts or components not supplied by REDYREF
    - o Commercial hardware products that use, or in which have been installed, products or components that have not been provided by REDYREF
- Products or Peripherals with missing or altered service tags or serial numbers;
- Products for which REDYREF has not received payment;
- Outdoor products that are specifically designed for customer or customer has added non-REDYREF; components that did not have third party environmental validation testing;

• Packing and Shipping Product or Part to REDYREF hardware depot;

• Normal wear and tear.

THE LIMITED WARRANTIES OF REDYREF (SELLER) SET FORTH ABOVE ARE IN LIEU OF ALL WARRANTIES, EXPRESS OR IMPLIED, AND ALL OTHER OBLIGATIONS OR LIABILITIES ON THE PART OF SELLER, WHICH NEITHER ASSUMES, OR AUTHORIZES, OTHERS TO ASSUME FOR IT, ANY OTHER OBLIGATION OR LIABILITY IN CONNECTION WITH THE WARRANTED WORK OR ANY OTHER PART THEREIN. PURCHASER HEREBY WAIVES SUCH OBLIGATIONS OR LIABILITIES OF SELLER, AS PART OF THIS AGREEMENT. THE SELLER HEREBY EXCLUDES FROM THIS WORK THE IMPLIED WARRANTY OF MERCHANTABILITY AND SELLER ALSO EXCLUDES THE IMPLIED WARRANTY OF FITNESS OF PARTICULAR PURPOSE FOR WORK HEREBY PERFORMED. IN NO EVENT WILL THE SELLER BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, SECONDARY, OR INCIDENTAL DAMAGES, FOR ANY REASON OR ARISING OR ASSOCIATION WITH, THE WORK PERFORMED HEREUNDER. IN NO EVENT SHALL THE SELLER'S LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL VALUE OF THE PARTICULAR ORDER.

5. PAYMENTS

5.1 Payment Terms. All amounts due and payable to REDYREF hereunder shall be remitted by Customer within thirty (30) days from the date of the applicable REDYREF invoice unless specified otherwise in 5.1.1 or 5.1.2 of this Agreement, REDYREF's Hosting Services Agreement, or as specified in each SOW/PROPOSAL. All payments are to be made in United States Dollars.

5.1.1 Annual Subscription / Transaction Processing Fees: REDYREF will invoice for license subscriptions and transaction fees as set forth in the SOW/PROPOSAL.

5.1.2 Other: REDYREF will invoice for all other services set forth in an SOW/PROPOSAL when applicable and will be due on the due date specified on the invoice.

5.2 Late Fees; Disputed Amounts. In the event of the Customer's payment is not received by the due date, Customer shall pay late fees equal to (i) one and one-half percent (1 ½%) of the unpaid balance then due for each thirty (30) day period or portion thereof that such balance remains unpaid; or (ii) the maximum rate permitted by Law if lower than the stated rate. Customer will bring any disputed amounts to REDYREF's attention in writing not more than 15 business days following receipt of an invoice from REDYREF. If Customer does not bring such a dispute to REDYREF's attention within that 15-business day period, REDYREF will treat that original amount as due and payable according to its original terms.

5.3 Taxes. The Fees set forth in each SOW/PROPOSAL are exclusive of any federal, state, provincial or local sales, use or excise taxes levied on or measured by the sale, sales price, or use of the Products and Services, but excluding any taxes on income, property, or operations (collectively, "Taxes"). If applicable, Customer shall provide REDYREF with evidence of any exemption from such Taxes. If Customer is unable to produce such evidence, the parties shall collect and remit Taxes, if any, as required by applicable law. Except as otherwise expressly stated on each SOW/PROPOSAL.

5.4 Expenses. Customer shall pay REDYREF, in addition to the quoted prices, all Expenses not included in SOW/PROPOSAL, reasonably incurred by REDYREF's employees in performing the work called for under Agreement(s), provided such Expenses were pre-approved by Customer and are clearly specified in the invoice and copies of receipt or other proof of the Expenses are attached thereto. Per diems or

other allowance shall be billed at REDYREF's standard time and material rate or as set forth in each SOW/PROPOSAL. REDYREF agrees to invoice the Customer for Expenses as incurred. Customer acknowledges that certain Expenses may track through REDYREF's accounting system on a delay basis and may be invoiced after completion of the contract services, provided that REDYREF shall not issue an invoice for expenses later than ninety (90) days after completion of contract services to which Expenses relate. Unless otherwise noted in the invoice, Expenses are payable within thirty (30) days after receipt of the invoice.

5.5 Suspension of Services and Delivery of Products. Except in the case of good faith disputes concerning the parties' obligations of performance, including without limitation payments due from Customer under any SOW/PROPOSAL, or in the absence of written notice with sufficient specificity and detail for REDYREF to understand the reasons for and to remedy a Customer dispute under an SOW/PROPOSAL, REDYREF may in its sole discretion withhold, delay or condition the delivery of or access to Products, Services, Client Software or Custom Work upon the resolution of such dispute (e.g., for Customer's failure to timely pay any such amounts due). Such action by REDYREF does not relieve Customer of its obligation to make payment or otherwise discharge its requirements under this Agreement.

5.6 Customer Acceptance. If an SOW/PROPOSAL provides specific criteria for acceptance or for specific acceptance testing of a Product or Custom Software as a precondition to the occurrence of Delivery (or the ability of REDYREF to invoice upon Delivery), Delivery is deemed to occur as to any Product upon acknowledgement by Customer that the Product successfully conforms to the acceptance criteria or the successful completion of testing. Customer shall commence any applicable evaluation for acceptance or acceptance testing promptly following REDYREF's notice that the Product is ready for such evaluation or testing. If Customer believes in good faith that Delivery has not occurred or that any applicable criteria or protocols have not been successfully achieved, Customer shall submit a written notice of rejection to REDYREF (with sufficient specificity and detail for REDYREF to understand the reasons for the rejection and to remedy such defects) within 15 business days following REDYREF's statement that the Product is ready for such evaluation or testing. REDYREF will promptly remedy any defects in Delivery for Product for which REDYREF is responsible. Acceptance shall occur if: (i) Customer accepts the Product in writing; (ii) Customer places the Product into general commercial service or makes commercial use thereof; (iii) the Product objectively passes acceptance testing; or (iv) more than 15 business days pass following the delivery of the Product or completion of any applicable acceptance evaluation or testing without REDYREF's receipt of the written notice from Customer described in this paragraph.

If REDYREF has arranged for shipping, REDYREF is not liable for any damage if Customer did not inspect shipment upon delivery. Customer must inspect and check the product prior to freight carrier leaving Customer facility. Customer must also mark bill of lading with any comments describing the damage. Customer is entitled to refuse shipment due to damage. If unsure what to do call REDYREF customer service department at 800-628-3603 x2 or email to support@redyref.com. If Customer has arranged for shipping, REDYREF is no liable for any damage. The risk of loss or denial of proper insurance coverage as a result of failure to adhere to these terms shall be borne by Customer.

If REDYREF has completed production of SOW/ PROPOSAL and Customer has delayed shipment for more than 60 days than REDYREF will invoice Customer for storage of Product based on storage fees listed on the SOW/Proposal.

6. TERM, OBLIGATIONS AND TERMINATION

6.1 Term. This Agreement shall become effective as of the effective date of the earliest SOW/PROPOSAL executed on or around the date of this Agreement and remain in effect until terminated in accordance with this Section 6 (the “Term”). Notwithstanding anything to the contrary, this Agreement will continue to apply to any SOW/PROPOSAL until that SOW/PROPOSAL is completed or properly terminated. If a SOW/PROPOSAL is for recurring or ongoing Services for a specific term, upon expiration of the initial term, such SOW/PROPOSAL will automatically renew for one or more additional terms for the same period as the initial term or then current term of the SOW/PROPOSAL unless either party notifies the other party in writing of its intent to terminate such SOW/PROPOSAL at least 30 days prior to the expiration of the then current term.

6.2 Termination. Provided neither party has any obligation of performance, Customer has paid in full for all work performed and all Deliverables have been provided under an outstanding SOW/PROPOSAL, either party may terminate this Agreement at any time upon 30 days’ written notice to the other party.

6.3 REDYREF Obligations. In conjunction with the obligations identified in Sections 6.3.1 and 6.3.2, REDYREF may host the Licensed Software for Customer and/or utilize a third-party payment processing solution. In such case, additional terms and conditions are detailed in REDYREF’s Hosting Services Agreement.

6.3.1 Administration: REDYREF will provide administration tools that will allow Customer to setup and configure the Licensed Software.

6.3.2 Limitations: Under the terms of this Agreement, REDYREF shall not take any responsibility for the service offered by Customer. REDYREF shall not be responsible for the daily administration of the content offered by Customer, unless requested by Customer and subject to applicable fees detailed in SOW/Proposal.

6.4 Indemnification by REDYREF. REDYREF agrees to indemnify, defend and hold harmless Customer, its parent companies and affiliates and their officers, directors, employees and agents of and from any and all liability, claims, liens, demands, actions and causes of action whatsoever arising out of or related to any loss, cost, expenses (including reasonable attorney’s fees), damage or injury arising as a result of the acts or omissions of REDYREF in connection with the services to be provided hereunder or a breach of this Agreement or negligence or willful misconduct by REDYREF.

6.5 Indemnification by Customer. Customer will indemnify, defend, and hold harmless REDYREF from and against any proceedings, claims, demands, expenses (including reasonable attorneys’ fees), or damages of any nature rising out of or in connection with Customer’s violation of the scope of the rights and licenses granted herein.

6.6 Subsequent Obligations. Prior to the effective date of termination of this Agreement, at Customer’s option, REDYREF agrees to offer Customer a license to the Software at the then current posted price for the same or equivalent functionality. Also prior to the effective date of termination, REDYREF will assist Customer in removing all of Customer’s data stored on REDYREF’s servers and in any related data or information required for Customer to run its operations on other servers. This assistance will be billed at the standard time and material rate or as set for in an SOW/PROPOSAL. After having provided Customer access and sufficient time to port its data to alternate servers, Customer’s access codes for the Hosted Licensed Software shall be terminated, and Customer and its authorized users shall thereupon have no further ability to access or use the Hosted Licensed Software or any data Customer may have stored in the REDYREF computing environment. REDYREF shall retain all data Customer has stored in the

REDYREF computing environment for a period of thirty (30) days after the effective date of any termination or expiration of this Agreement, and so long as Customer has paid all amounts due to REDYREF in accordance with Section 5, Upon the expiration of such thirty (30) day period, REDYREF shall purge all Customer data from the REDYREF computing environment.

6.7 Effect of Termination. Upon expiration or notice of termination of this Agreement for any reason, all Fees and other charges under this Agreement (and all applicable SOW/PROPOSAL's) will be immediately due and payable, all licenses granted pursuant hereto shall immediately terminate (except as provided in Section 2.F.), and each party shall return to the other all property (including any Confidential Information) of the other party in its possession or control. REDYREF will promptly cease performing all Services and all Customer access to the Services shall be immediately suspended.

7. INSURANCE.

7.1 Insurance Requirements. REDYREF shall obtain and maintain in force the following insurance coverage covering the activities under this Agreement during the Term of this Agreement:

A. Workers' Compensation Insurance. REDYREF shall maintain workers' compensation insurance with a minimum of $1,000,000.00 Employers Liability; and

B. Automobile Liability Insurance. REDYREF shall maintain automobile liability insurance of $1,000,000.00 combined single limit for any one accident covering any auto whether owned, non-owned and hired; and

C. Commercial General Liability Insurance. REDYREF shall maintain commercial general liability insurance with a combined single limit of $1,000,000.00 per occurrence for bodily injury, personal injury and/or property damage liability. If such policy includes a General Aggregate limit then the General Aggregate limit shall not be less than $5,000,000.00; and

D. Professional E&O Insurance. REDYREF shall maintain professional E&O insurance with a combined single limit of $1,000,000.00 per occurrence.

For all policies, REDYREF agrees to have insurer provide thirty (30) days prior written notice of cancellation, non-renewal or modification of coverage to Customer. REDYREF further agrees that it will name Customer and its parent, subsidiary and affiliated companies and the officers, directors, agents, shareholders and employees of each as additional insured (together the "Additional Insureds") in its commercial general liability policy. REDYREF shall submit any and all appropriate insurance certifications to Customer evidencing coverage, limits and naming the Additional Insureds.

8. MISCELLANEOUS PROVISIONS

8.1 Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, REDYREF'S AGGREGATE LIABILITY FOR CLAIMS RELATING TO OR ARISING OUT OF SERVICES PROVIDED WHETHER FOR BREACH OF CONTRACT, IN TORT, OR UNDER ANY OTHER LEGAL THEORY, IS LIMITED TO THE FEES PAID HEREUNDER BY CUSTOMER. IN NO EVENT WILL REDYREF BE LIABLE FOR ANY INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH OR ARISING OUT OF THIS AGREEMENT (INCLUDING LOSS OF BUSINESS, REVENUE, PROFITS, USE, DATA OR OTHER ECONOMIC ADVANTAGE), HOWEVER CAUSED AND REGARDLESS OF THE LEGAL THEORY OF LIABILITY, EVEN IF REDYREF HAS BEEN ADVISED OF

THE POSSIBILITY OF SUCH DAMAGES, AND EVEN IF ANY EXCLUSIVE REMEDY PROVIDED FOR HEREIN FAILS OF ITS ESSENTIAL PURPOSE.

8.2 Force Majeure. If either party is unable to perform any of its obligations under this Agreement because of natural disaster, pandemics, actions or decrees of governmental bodies, communications line failure not the fault of the affected party, or other event beyond the reasonable control of the affected party (a “Force Majeure Event”), the party who has been so affected shall immediately give notice to the other party and shall do everything possible to resume performance. Upon receipt of such notice, all obligations under this Agreement shall be immediately suspended for the duration of the Force Majeure Event.

8.3 Relationship of the Parties. This Agreement does not constitute either party the agent of the other, or create a partnership, joint venture or similar relationship between the parties or Third-Party Sellers, and neither party nor Third-Party Sellers will have the power to obligate the other in any manner whatsoever.

8.4 Amendments. No amendments, modifications, or supplements to this Agreement shall be binding unless they are in writing and signed by both parties hereto.

8.5 Counterparts; Email. This Agreement may be executed in one or more counterparts, each of which when so executed shall be an original, but all of which together shall constitute one agreement. This Agreement may be executed by email signature.

8.6 Governing Law. This Agreement shall be construed and interpreted in accordance with the laws of the State of New Jersey.

8.7 Joint Marketing. REDYREF may use Customer’s name in a listing of new, representative, or continuing customers in press releases, on its website, or in other marketing materials or dissemination of information. The parties may agree to cooperate in joint marketing activities or in issuing a joint press release at the request of either party, subject to prior written consent and approval of the form and substance by both parties.

8.8 Non-Solicitation. During the Term and continuing until the first anniversary of the expiration or termination of this Agreement, each party shall not and shall ensure that its affiliates do not, directly, or indirectly, solicit or attempt to solicit for employment any persons employed or contracted by the other party.

8.9 Assignment. Either party may assign this Agreement without the other party’s prior written consent to a successor in interest in the event of a merger, sale of all or substantially all of the assets of such party, or consolidation; provided, however, that the surviving entity or purchaser expressly assumes in writing the performance of all of the terms of this Agreement. This Agreement is binding upon, inures to the benefit of and is enforceable by the parties hereto and their respective successors and assigns.

IN WITNESS WHEREOF, the parties, by their duly authorized representatives, have executed this Agreement as of the Effective Date.

“REDYREF”	**“Customer”**
EVS Interactive, Inc.	_____
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

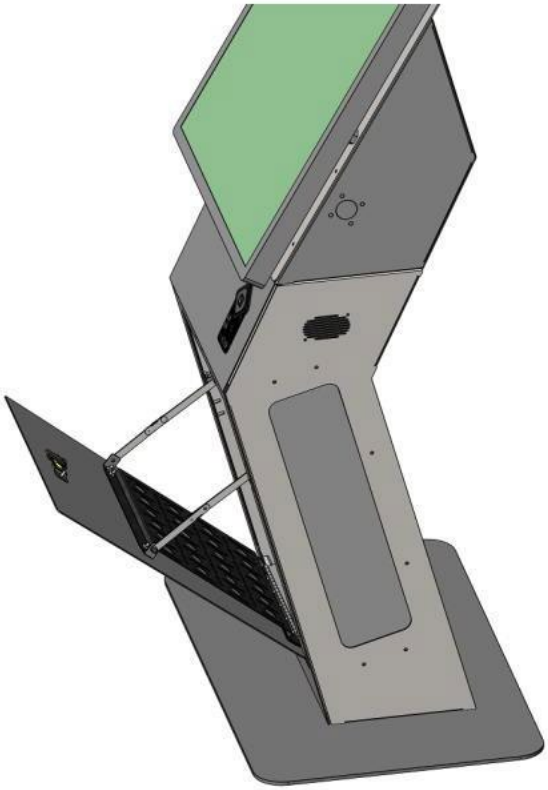
Appendix C. Redyref Owner's Manual

The following text is from the User Manual provided by Redyref.

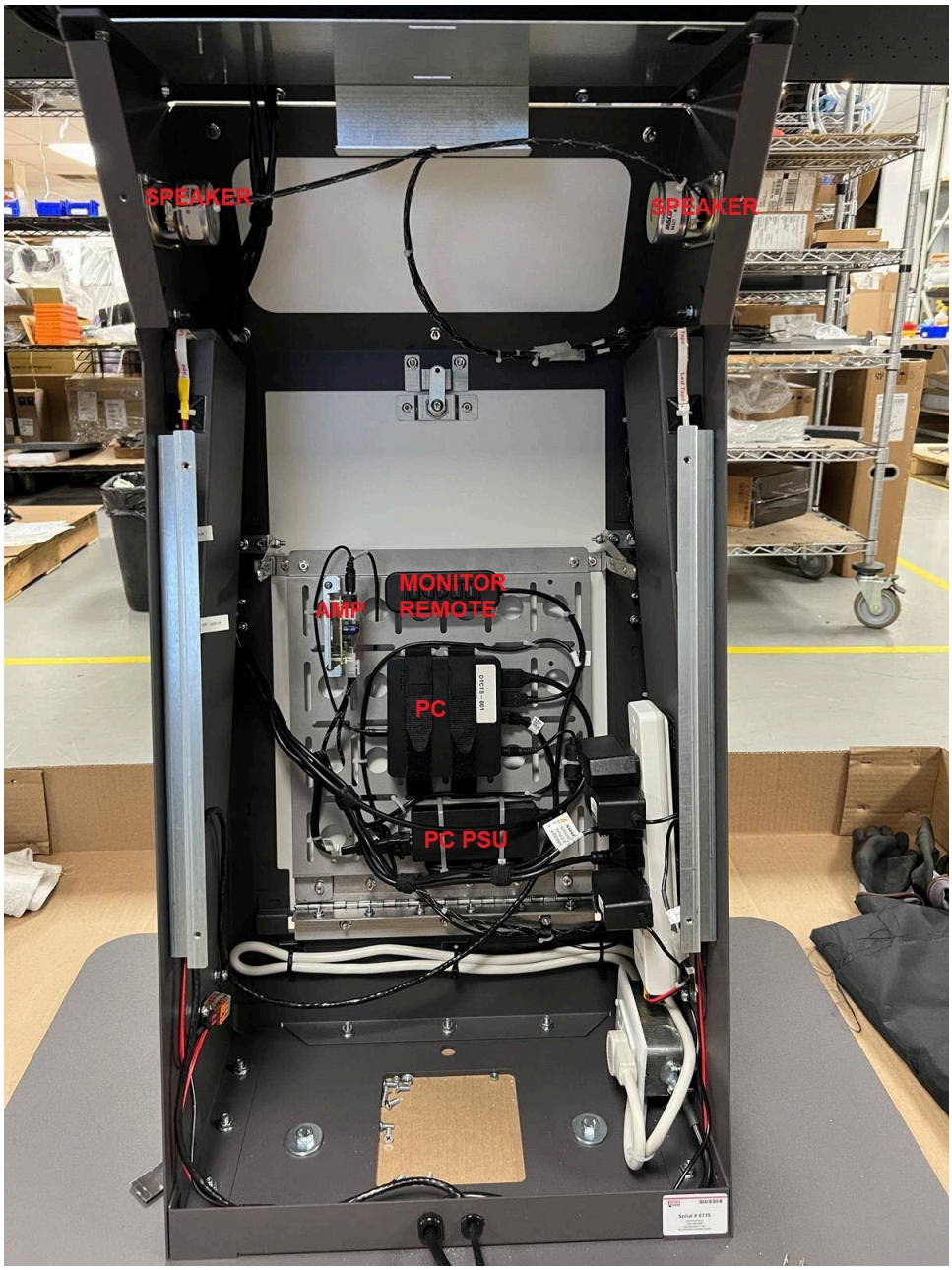
Owner's Manual

Closed View

Open View



Notated View



WARRANTY Does Not Cover:

- Software not provided by REDYREF, including without limitation, the operating system and software added to the REDYREF-manufactured hardware products through our factory-integration system, third-party software or the reloading of software
- Non REDYREF-provided products and accessories
- Problems that result, directly or indirectly, from:
    - External causes such as accident, abuse, misuse, vandalism or problems with electrical power.

  - Improper ventilation.
  - Servicing not authorized by REDYREF.
  - Usage that is not in accordance with product instructions.
  - Failure to follow the product instructions or failure to perform preventive maintenance.
  - Using accessories, parts or components not supplied by REDYREF.
  - Commercial hardware products that use, or in which have been installed, products or components that have not been provided by REDYREF.
- Products or Peripherals with missing or altered service tags or serial numbers
- Products for which REDYREF has not received payment.
- Outdoor products that are specifically designed for customer or customer has added non-REDYREF components that did not have third party environmental validation testing.
- Normal wear and tear.

Maintenance (Cleaning):

In order to keep your kiosk looking its best, general maintenance will be required. General cleaning of the kiosk can help prevent operation issues down the line as well. **TURN OFF POWER SWITCH BEFORE PERFORMING MAINTENANCE.** Follow the guidelines below to keep your kiosk clean and running smoothly:

● **Kiosk Enclosure**: Use a cloth with rubbing alcohol to wipe down the kiosk enclosure (interior and exterior). Be sure to be careful not to touch the screen with the rubbing alcohol.

● **Touchscreen Display**: Use a cloth with Windex or a comparable product (DO NOT spray the Windex directly onto the screen) to wipe down the screen display, removing any dust, smudges or fingerprints. **NEVER** use alcohol or solvent based products to clean the screen.

● **Fans**: If possible, use compressed air to remove any dirt/dust from the fans. If compressed air is not available, a cloth may be used.

● **Kiosk Interior**: It is recommended to clean the interior of the kiosk (all components) with compressed air to remove any dust inside. Dust build up can interfere with the functionality of components within the kiosk.

● **Replacing Filter:** Refer to "Filter Replacement Instructions" document.

Operations:

● Doors:

○ Use the provided keys to unlock/lock the doors to the kiosk.

○ Ensure there is nothing between the cabinet and the door before locking.

● Monitor:

○ The monitor brightness may be adjusted in the settings menu via the remote.

○ Contact support@redyref.com for assistance.

● Computer:

○ To turn off, hold down power button for 5 seconds.

○ To turn on, tap the power button. There should be an LED that indicates power is going to the PC.

● Amplifier

○ To turn off, unplug the power cable from the amplifier.

○ To turn on, plug the power cable back into the amplifier

○ To adjust volume, turn the volume dial up or down.

Support:

● If there are any issues with the functionality of this kiosk or replacement parts are needed, please contact **support@redyref.com**

● When experiencing issues with a component (i.e.. Monitor, PC, etc.) try disconnecting, then reconnecting the cables and restarting the device before contacting support.

U.S. Department of Transportation
ITS Joint Program Office – HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487

www.its.dot.gov

FHWA-JPO-23-107

U.S. Department of Transportation