Phase 2 Data Privacy Plan (DPP)

Georgia Department of Transportation: Safe Trips in a Connected Transportation Network ITS4US Deployment Project

www.its.dot.gov/index.htm

Final Report — August 29, 2023
FHWA-JPO-22-970

ITS4US

IT'S TRANSPORTATION FOR ALL OF US

U.S. Department of Transportation

Produced by Georgia Department of Transportation (GDOT)
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-22-970		

4. Title and Subtitle	5. Report Date
Phase 2 Data Privacy Plan (DPP) Safe Trips in a Connected Transportation Network ITS4US Deployment Project	August 29, 2023
	6. Performing Organization Code (Delete and insert information here or leave blank)

7. Author(s)	8. Performing Organization Report No.
Kofi Wakhisi (ARC), Bennet Foster (ARC), Randall L. Guensler (Georgia Institute of Technology), Angshuman Guin (Georgia Institute of Technology), Polly Okunieff (GO Systems and Solutions), Natalie Smusz-Mengelkoch (ICF)	(Delete and insert information here or leave blank)

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Georgia Department of Transportation – One Georgia Center 600 West Peachtree NW, Atlanta, GA 30308	**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
	14. Sponsoring Agency Code HOIT-1

15. Supplementary Notes

The following USDOT partners are supporting this document development: Elina Zlotchenko (Program Manager), Sarah Tarpgaard (Agreement Officer), and Norah Ocel (Agreement Officer Representative)

16. Abstract

The Georgia Department of Transportation ITS4US Deployment project, Safe Trips in a Connected Transportation Network (ST-CTN), is leveraging innovative solutions, existing deployments, and collaboration to make a positive impact using transportation technology to support safety, mobility, sustainability, and accessibility. The ST-CTN concept is comprised of an integrated set of advanced transportation technology solutions (connected vehicle, transit signal priority, machine learning, predictive analytics) to support safe and complete trips, with a focus on accessibility for those with disabilities, older adults, and those with limited English proficiency.

The Data Privacy Plan (DPP) highlights the data privacy controls and measures used by the project team to mitigate risk of harming individuals as a result in the improper handing or disclosure of the Personally Identifiable Information (PII) or Sensitive Personally Identifiable Information (SPII) collected from individuals in connection with the ST-CTN Project. The document reviews the access requirements for data entering and exiting the system with a specific focus on specifically personally identifiable information (PII). The document describes the data assessments used to ensure traveler privacy. These assessments consider the potential risks and mitigation strategies as well as security controls developed to maintain a secure and private environment for all end users.

17. Keywords	18. Distribution Statement
ITS4US; Deployment; ITS; Intelligent Transportation Systems; Safe Trips in a Connected Transportation Network; Participant Training; Stakeholder Education; Data Privacy Plan	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	(51)	**N/A**

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Revision History

Name	Date	Version	Summary of Changes	Approver
GDOT Team	17 July 2023	0.1	Draft Phase 2 Document	Bennett Foster
GDOT Team	14 August 2023	0.2	Draft Final Phase 2 Document	Bennett Foster
GDOT Team	29 August 2023	1.0	Final Phase 2 Document	Bennett Foster

PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Document Purpose

The Phase 2 Data Management Plan (DMP) provides an inventory of the datasets and their characteristics related to the GDOT ITS4US project – ST-CTN. The inventory includes datasets that are ingested, generated, processed, and exported by the ST-CTN system including static, real-time, and archived datasets. The plan includes information on data governance, management, security and privacy policies, storage, and access, as well as the relationship of the data to performance measures.

The Data Privacy Plan (DPP) is related to the DMP and describes the privacy and security needs of the ST-CTN project to protect user privacy and mitigate risk of threat to users, data privacy, and system hardware. The DPP includes information specific to private data as it relates to access requirements, risk assessment, and security policies and procedures.

1.1.1 Organization of this Document

The document includes the following sections:

Section 1: Introduction provides a description of the document purpose and deployment concept.

Section 2: Privacy Approach describes all data access requirements needed to meet user needs, security assessment processes, data security requirements for each dataset, and an assessment of the likelihood and impact of all data privacy risks for the project. This section will also discuss the data sharing and provision process and an analysis of all key system hardware components and their security concerns.

Section 3: Security Controls identifies the technical and policy controls used to support the data privacy requirements for the ST-CTN system.

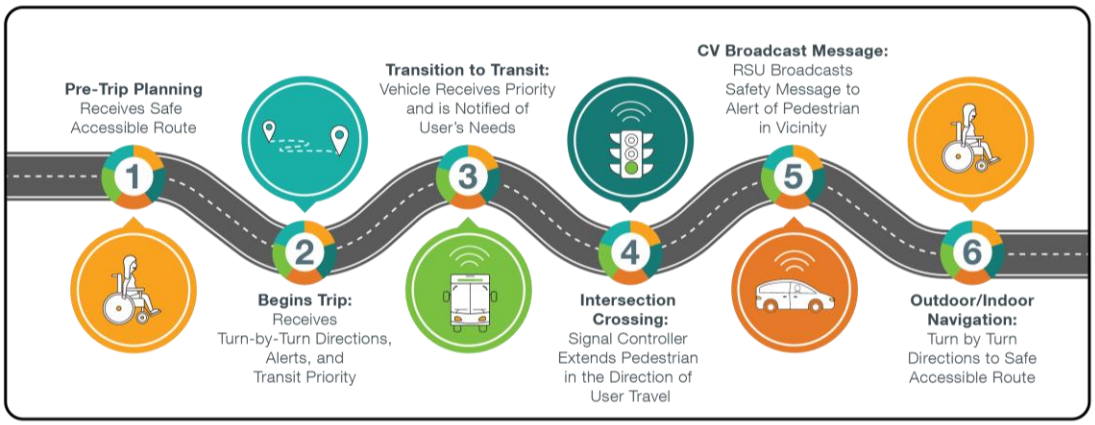
Appendix A: Acronyms and Glossary includes tables that list the acronyms and terms used throughout this document.

Appendix B: References lists the documents referenced throughout this document.

1.2 Deployment Concept

The ST-CTN project aims to upgrade and integrate existing technologies and services to assist underserved populations with completing their complete trip successfully, safely, and reliably. The vision of the project is to provide users complete trip functionality with directions, conditions, and status on the links between trip legs that are personalized based on the user's profile, while connecting the user to CV infrastructure to provide safer trips and more transportation network

awareness. As an illustration of how the ST-CTN system will be used, transit-based trips were delineated into six segments (as depicted in **Figure 1**) to allow for easier understanding and a greater breakdown of priorities and goals.



Source: ARC, 2020

Figure 1. Traveler's Complete Trip

The delineated trip segments include the following steps and project components:

- **Step 1 Pre-Trip Planning.** The traveler plans for and receives a safe accessible route.
    - The ability to customize trip preferences based on the user's abilities.
- **Step 2 Begins Trip.** The traveler begins their trip and receives turn by turn directions, alerts, remote pedestrian activation, and can trigger transit signal priority (TSP) if the user requires additional time boarding or alighting a transit vehicle, is unable to stand for long periods, or is sensitive to weather conditions.
    - Turn by turn, shortest path, directions along pathways that meet user defined preferences.
    - Provides support services for users if they become disoriented or have issues accessing defined paths.
    - Activates TSP for buses if the user requires additional time boarding or alighting a transit vehicle, is unable to stand for long periods, or is sensitive to weather conditions.
- **Step 3 Transition to Transit.** The traveler transitions to transit and the transit vehicle receives priority and is notified of users' needs. TSP can be triggered if the bus is running behind schedule due to a longer boarding time needed by a user.
    - Provides users with transit trips that have accommodations that meet user defined preferences.
    - Sends alerts to transit vehicles when users need additional time to board, navigate internally, or alight the transit vehicle.
    - Remotely requests service from transit vehicles while waiting to board or alight.
    - Triggers TSP if the bus is running behind schedule due to a user needing additional time to board or alight.

- **Step 4 Intersection Crossing.** When crossing a signalized intersection, the traveler indirectly interacts with the signal controller in that an authorized system call is made to the controller which extends the pedestrian phase in the direction of user travel.
    - Allows the user to communicate with connected intersections if they are unable to reach or press the crosswalk button.
    - Provides the user with information about the intersection crossing and adds time to the crossing if needed.
- **Step 5 CV Broadcast Message.** Roadside units (RSUs) broadcast safety message to alert CVs of pedestrians in the intersection.
    - Provides the ability for users to remotely request service from transit vehicles while waiting to board or alight.
    - Provides communications to CVs from pedestrian crossing signal system (via RSUs) to make them aware of pedestrians crossing a roadway.
    - Provides communications between transit vehicles and travelers waiting at a transit stop to make them aware of each other.
- **Step 6 Outdoor/Indoor Navigation.** The traveler is provided with turn-by-turn directions to a safe accessible route.
    - Hands-free navigation via mobile apps and/or wearables and accessible channels (haptic, voice, text).
    - Alerts and dynamic rerouting in response to changes in path conditions.
    - Provides the user with accessible routes into and through transit hubs within the project area.
    - Provides users with updates on the operating status of indoor infrastructure such as elevators and escalators.

System development and system integrations completed within the scope of this project will enable travelers – specifically those in the underserved community – to program and safely complete single mode or multimodal trips that are based on their abilities; improve the transition between modes by providing additional details to users and transit service operators; suggest dynamic routing changes based on infrastructure condition and calculated delay.

The existing initiatives that are being leveraged to support the proposed ST-CTN system are defined in more detail below as well as those components that will be developed specifically to support ST-CTN project evaluation. The icons and colors depicted below are used throughout the DPP to clearly identify the critical components of ST-CTN. In some cases, partner agencies are upgrading the services within their current systems to create a more robust dataset or toolset for the ST-CTN program.

OTP for G-MAP. Atlanta Rider Information and Data Evaluation System (ATL RIDES) includes an Open Source Software (OSS) multi-modal trip planning and mobile application, integrated mobile fare payment options, and a Connected Data Platform (CDP) using regional General Transit Feed Specification (GTFS) transit service data. The tool supports multi-agency context, multilingual support, and mobile app turn-by-turn directions. The OpenTripPlanner (OTP) architecture facilitates integration with additional OSS tools including a data analytics engine, call center module with application programming interfaces (APIs), and

account management system. The existing ATL RIDES application will be modified and enhanced based on ST-CTN project needs and leveraged to create a new, independent application which will be differentiated as the *OTP for G-MAP* subsystem (hereafter referred to as G-MAP).

SIDEWALKSIM. SidewalkSim is an asset management system and shortest path (lowest impedance) routing tool for pedestrian pathways. Site inspections provide more detailed ADA and inclusive design and condition data for use in pathway accessibility analysis. SidewalkSim identifies the best path between any two points in the pedestrian network, given the set of pathway characteristics and any user-specified needs and route penalties.

CV1K. The Atlanta region is home to one of the largest CV deployments in the United States – Regional Connected Vehicle Infrastructure Deployment Program (CV1K). CV1K is deploying interoperable CV technologies at signalized intersections throughout the Atlanta region using both Dedicated Short-Range Communications (DSRC) and Cellular Vehicle to Everything (C-V2X) technologies to deliver safety and mobility-based applications. The program provides support to configure, operate, and maintain CV infrastructure and applications, including TSP. Gwinnett County is one of the largest recipients of the first phase of this deployment.

CVTMP. Gwinnett County's Connected Vehicle Technology Master Plan (CVTMP) sets out to develop and improve economic viability and quality of life, address the needs and challenges to motorized and non-motorized modes, establish guidelines for deploying technology, and have broad applicability to Gwinnett, other local jurisdictions, and across the state—to set the standard for implementing CVs. Among the high priorities is establishing a mobile accessible safety program and alternative strategies for TSP in Gwinnett County.

STM. The Space Time Memory (STM) platform processes traffic volume and speed data from multiple monitoring and modeling sources, tracks network performance measures, and predicts evolving route conditions using traditional and machine learning techniques. The STM projects trip trajectories through the transportation network, as network conditions change in space and time. This tool will be applied to analyze and predict performance through the multi-modal transportation network. The shortest path analysis will be applied to the combined roadway, transit, sidewalk, and shared-use path networks, allowing routing decisions to incorporate travel time, safety, and other impedances into path selection.

PMD. The Performance Measurement Dashboard (PMD) is a data storage and distribution tool that archives operational, survey and performance metrics of the system. The PMD is envisioned to ingest, quality check, and curate all types of data – static and dynamic, structured and unstructured, open and private datasets. The PMD will store the datasets so that they can be viewed and accessed based on user roles. The PMD will include a public PMD for the public to access open data presented on an interactive dashboard to the public.

2 Privacy Approach

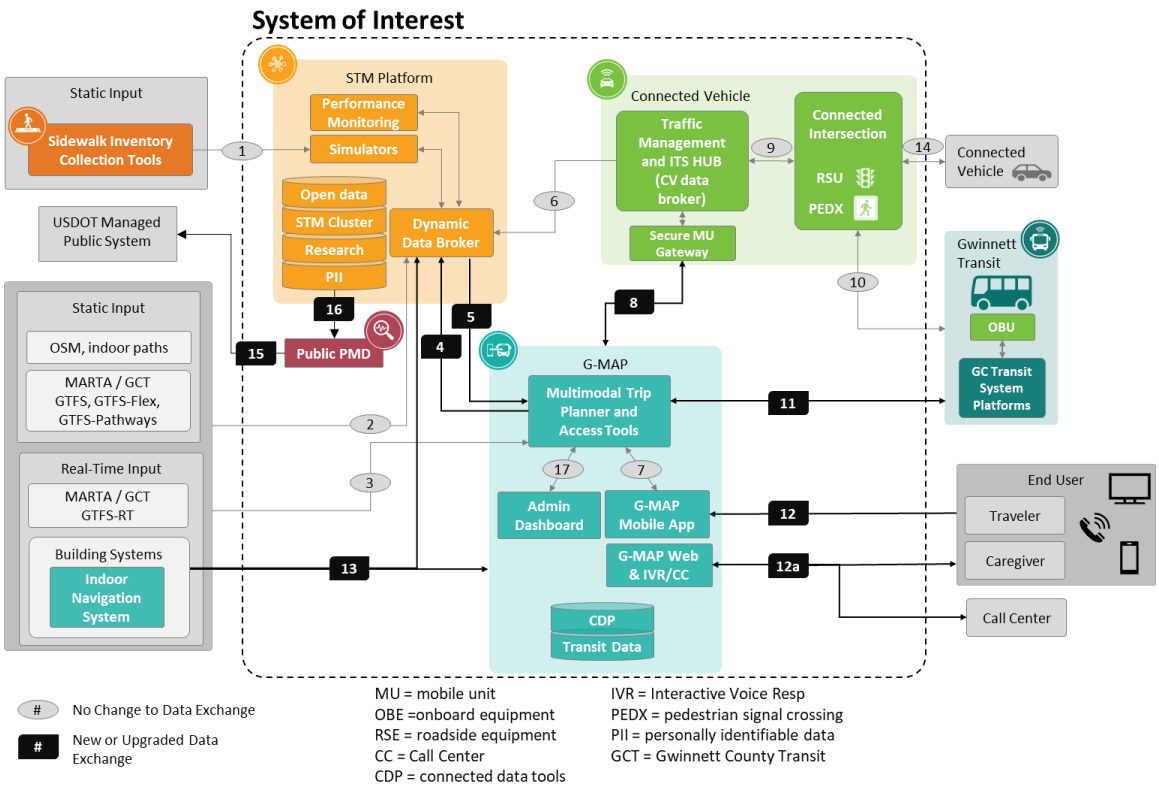
The approach to ensuring the privacy of the ST-CTN system data is described within the context of securing and protecting access to the data. Data access levels are differentiated by proprietary data which are restricted by license or usage agreements versus protected datasets that require access controls to preserve privacy and security. The following sections provide a summary of the data and the approach to ensuring the privacy and security of the *private* datasets.

2.1 System Data Summary

The ST-CTN can be thought of as a *system of systems.* The scope of work required to develop, design, and deploy ST-CTN is focused on the expansion or enhancement of current systems and added connectivity between those systems.

Figure 2 provides a context diagram of the proposed system – indicating the system of interest and added subsystem connectivity.

Critical ST-CTN data exchanges entering and exiting the system are identified by number and color in the context diagram and correspond to the exchanges described in **Table 1**. These descriptions are focused only on the scope of work required to implement the new system and information that is necessary to provide context to that work. As described in **Section 1.2**, there are a number of existing and on-going efforts that are being performed outside the scope of this project that are critical to the success of ST-CTN.



Source: GDOT, 2023

Figure 2. Data Flow / Functional Architecture for ST-CTN System

The system information flows (or exchange identifications, EX IDs) are identified by number in the functional diagram above and described in **Table 1**. The grey oval labels indicate existing data exchanges that will be utilized with no change to the current data exchange. Black rectangular labels indicate data exchanges that will be new or upgraded to support the ST-CTN system. The source and destination of each information flow is defined.

Table 1. Critical ST-CTN Information Flow Descriptions

EX ID	Description	Source	Destination
1	Sidewalk inventory data, including accessibility features to the STM Platform simulators	External	STM
2	Static data from various existing sources to the STM Platform dynamic data broker and G-Map OTP Network and other tools including GTFS, OSM, Indoor pathways	External	G-MAP, STM
3	Dynamic or realtime data from various existing sources to the STM Platform dynamic data broker and G-Map Middleware	External	G-MAP, STM
4	G-MAP Mobile App logs and trip feedback	G-MAP	STM

EX ID	Description	Source	Destination
5	STM Network Impedance API	STM	G-MAP
6	CV and Traffic Operations Messages: signal phasing and timing road characteristics, traffic data	CV	STM
7	Open Trip Planner (OTP) APIs and G-MAP APIs	G-MAP (trip planner)	G-MAP (channel access)
8	Mobile Accessible Pedestrian Signal System (PED-SIG)	G-MAP	CV (Secure MU gateway)
9	CV messages includes PSM, BSM and other CV messages and Signal Controller monitoring and control information	CV	CV Connected Intersection
10	Transit signal priority (TSP) and other CV application messages	Ride Gwinnett OBU	CV Connected Intersection
11	Ride Request messages	G-MAP Mobile App via G-MAP	Gwinnett Transit
12	G-MAP Mobile App APIs and Traveler exchange – profile, trip plan, settings, notifications, feedback, etc.	G-MAP	G-MAP Mobile App
12 A	G-MAP Call Center and Trusted Companion – profile, trip plan, settings, feedback (subset of information exchanges tailored for website, call takers and caregivers)	G-MAP	Website, Call Center, Caregiver device
13	Dynamic information from building facilities, including beacon signals to the G-MAP Mobile App	Building System (external)	G-MAP Mobile App
14	CV data (i.e., BSMs)	CV OBU	CV RSU
15	Project data for USDOT-managed Public System	Public PMD	USDOT Managed Public System
16	Public facing data and visualizations for reporting on system operations and performance	Private PMD (STM)	Public PMD
17	G-MAP Administration Tool configuration and control message exchanges	G-MAP	G-MAP

Data is exchanged within the information flows identified above and the approach to privacy is determined by the defined access level.

2.2 Access Requirements

Access to ST-CTN project data is managed based on established requirements for each access level. Data access levels are defined as:

- **Open** – Data that can be used by the public with no or limited licensing restrictions. This data is available to the public without needing to request permissions and will be provided to the USDOT-managed Public System. These will be anonymized or aggregated versions of private datasets to protect PII.
- **Private** –Access to these data is limited and only granted with Institutional Review Board (IRB) and Project Team approvals. Subcategories:
  - **Operational** – real-time and other data used in the applications and operations of the system. The data may contain licensed data restricted by usage agreements.
  - **Proprietary –** Licensed data from third parties or commercial business interests (CBI). This data may be used for planning or operational purposes. Any access to the data is determined by usage agreements between the parties.
  - **Research** – Data that is available for research, but users of the data must meet IRB requirements before gaining access to the data. These datasets may have PII. These datasets are compiled for machine learning and research purposes that do not contain PII.
  - **PII Certification** – Data that has PII included in the dataset. The access to this data is as restrictive as possible to protect the PII based on IRB-approved processes. Data in this category should have an operational purpose that justifies its storage.

USDOT will be provided access to open data available through the USDOT-managed Public System and Public PMD which will include anonymized or aggregated versions of private datasets to protect PII. Security controls and technical access controls are described in **Section 3.1.1**.

2.3 Security Assessments

- The restriction of datasets occurs on two levels: *proprietary* datasets constrained by license agreements and *protected* datasets that are restricted because they contain PII.

Table 2 describes the classification of every dataset as Protected, Proprietary, or Open and identifies the basis for private data security assessment.

All proprietary data are stored on the secure server and working datasets are generated to which access is limited to project-specific modeling and data processing routines. Licensed data may be made available by the data owners to third parties. Most agencies that limit access to their data require the execution of a data user agreement to ensure data integrity and track data usage (at

no fee). Data licensed from private companies generally contains intellectual property and commercial value. Access to these data typically requires the execution of a data license and fees are likely required to obtain data access. Use of private data is minimized in this project, with the focus being on the use of open data.

The datasets are described by the following columns:

- **Dataset Identifier (ID):** unique identifier related to every dataset or dataset subset.
- **Information Flow / Exchange Identifier (EX ID):** unique identifier related to the information flow (**Figure 2**) that is utilized to exchange data.
- **Dataset Name:** the name or title for the dataset.
- **Access Levels:** describes how individuals may gain access or how the datasets may be used. Values include: PII Certified, Research, Proprietary, Operational and Open.
- **Reason(s) Data is Private:** describes why the data is designated as proprietary or protected. General reasons are stated above.

Table 2. Private Datasets

Data ID	EX ID	Dataset Name	Access Level	Reason(s) Data are Private
3	2	Whole Road Network	Open	NA
5	5	STM Network	Open	NA
8	2, 3	OSM Network	Open	NA
10	1	Sidewalk Network	Open	NA
11	1, 13	Indoor Pathways	Open	NA
15	2, 3	NaviGAtor Data	Operational	Subject to GDOT usage agreement.
20	2	Modeled Future Operating Conditions	Research / Proprietary	Derived from proprietary data sources.
25	5	Network Impedance API	Operational; Open	NA
26	1	Roadway Design and Condition Data	Open	NA

Data ID	EX ID	Dataset Name	Access Level	Reason(s) Data are Private
27	1	Roadway Intersection Design and Condition Data	Open	NA
29	1	Pedestrian Intersection and Pathway Asset Design and Condition Data	Operational	Subject to agency data license and usage restrictions.
30	13	Building Pathway Asset Design and Condition Data	Open	NA
31	13	Building Wayfinding Asset Design and Condition Data	Open	NA
32	2, 3	Transit Stop Asset Design and Condition Data	Open	NA
33	2, 3	Transit Vehicle Asset Design and Condition Data	Operational	Subject to agency data license and usage restrictions.
34	2, 3	GTFS (Ride Gwinnett)	Open	NA
35	2, 3	GTFS (MARTA)	Open	NA
36	2, 3	GTFS Realtime (Ride Gwinnett)	Open	NA
37	2, 3	GTFS Real-time (MARTA)	Open	NA
39	15	BSM	Operational	NA
44	8	Ped-X	Operational	NA

Data ID	EX ID	Dataset Name	Access Level	Reason(s) Data are Private
45	12	Trip options	Operational (real-time, transmitted, deleted), PII Certification (raw data)	Customer names and other traveler destinations such as home/work locations, and daycare/school locations, all constitute PII. Turn-by-turn directions reveal address locations.
46	2	VRU Categories	Open	NA
51	4	Mobile App Logs	PII Certification (raw data); Open (when PII is removed)	Customer names and other sensitive trip-related data (e.g., home/work locations, healthcare visits and daycare/school locations), all constitute PII. Trip logs reveal address locations.
52	4	Traverse Data	PII Certification	Customer names, home/work locations, and daycare/school locations, all constitute PII. Traverse data reveal address locations.
53	4	Trip Feedback Reports	PII Certification (raw data); Open (when PII is removed)	Customer names, home/work locations, and daycare/school locations, all constitute PII. Trip logs reveal address locations.
58	16	ST-CTN Performance Measures Data	Open	NA
59	16	STM Communication Logs	Open	NA
60	16	STM Impedance Calculation Logs	Open	NA
64	2	Ridership: Fixed Route	Open	NA

Data ID	EX ID	Dataset Name	Access Level	Reason(s) Data are Private
65	2	Ride Gwinnett Complaint Log	Research	The data contain data that must be secured.

2.3.1 Confidentiality, Integrity, and Availability (CIA) Assessment

Data security is commonly assessed by considering confidentiality, integrity, and availability (CIA) where the [NIST-3] defines the following:

- Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity — guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.
- Availability – ensuring timely and reliable access to and use of information.

Table 3 provides a summary of the CIA assessment prepared for the ST-CTN project. This assessment was conducted consistent with the [NIST-1] which define the potential confidentiality, integrity, and availability impact as follows:

- Confidentiality
    - Low - the unauthorized disclosure of information could be expected to have a **limited** adverse effect on organization operations, organizational assets, or individuals.
    - Moderate – the unauthorized disclosure of information could be expected to have a **serious** adverse effect on organization operations, organizational assets, or individuals.
    - High - the unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organization operations, organizational assets, or individuals.
- Integrity
    - Low - the unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organization assets, or individuals.
    - Moderate - the unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organization assets, or individuals.

- High - the unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organization assets, or individuals.

- Availability
  - Low – the disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
  - Moderate – the disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
  - High – the disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

In addition, the National ITS Reference Architecture – Security documentation was used to guide the security class assignment as shown below. Security class ranges from Class 1 to Class 5, with Class 1 being the least restrictive and Class 5 designating a need for higher security and controls [USDOT-1].

Table 3. CIA Assessment

Data ID	Dataset Name	Access Level	Confidentiality	Integrity	Availability	Security Class
3	Whole Road Network	Open	Low	Moderate	Moderate	1
5	STM Network	Open	Low	Moderate	Moderate	1
8	OSM Network	Open	Low	Moderate	Moderate	1
10	Sidewalk Network	Open	Low	Moderate	Moderate	1
11	Indoor Pathways	Open	Low	Moderate	Moderate	1
15	NaviGAtor Data	Open	Low	Moderate	Moderate	1
20	Modeled Future Operating Conditions	Research / Proprietary	Low	Moderate	Moderate	1

Data ID	Dataset Name	Access Level	Confidentiality	Integrity	Availability	Security Class
25	Network Impedance API	Operational; Open	Low	Moderate	Moderate	1
26	Roadway Design and Condition Data	Open	Low	Moderate	Moderate	1
27	Roadway Intersection Design and Condition Data	Open	Low	Moderate	Moderate	1
29	Pedestrian Intersection and Pathway Asset Design and Condition Data	Operational	Low	High	Moderate	3
30	Building Pathway Asset Design and Condition Data	Open	Low	Moderate	Moderate	1
31	Building Wayfinding Asset Design and Condition Data	Open	Low	Moderate	Moderate	1
32	Transit Stop Asset Design and Condition Data	Open	Low	Moderate	Moderate	1
33	Transit Vehicle Asset Design and Condition Data	Operational	Low	Moderate	Moderate	1
34	GTFS (Ride Gwinnett)	Open	Low	Moderate	Moderate	1
35	GTFS (MARTA)	Open	Low	Moderate	Moderate	1

Data ID	Dataset Name	Access Level	Confidentiality	Integrity	Availability	Security Class
36	GTFS Realtime (Ride Gwinnett)	Open	Low	Moderate	Moderate	1
37	GTFS Real-time (MARTA)	Open	Low	Moderate	Moderate	1
39	BSM	Operational	Low	Moderate	Moderate	1
44	Ped-X	Operational	Low	Moderate	Moderate	1
45	Trip options	Operational (real-time, transmitted, deleted), PII Certification (raw data)	High	High	Moderate	4
46	VRU categories	Open	Low	Moderate	Moderate	1
51	Mobile App Logs	PII Certification (raw data); Open (when PII is removed)	High	Moderate	Moderate	3
52	Traverse Data	PII Certification	High	Moderate	Moderate	3
53	Trip Feedback Reports	PII Certification (raw data); Open (when PII is removed)	High	Moderate	Moderate	3
58	ST-CTN Performance Measures Data	Open Data	Low	Moderate	Moderate	1
59	STM Communication Logs	Open Data	Low	Moderate	Moderate	1

Data ID	Dataset Name	Access Level	Confidentiality	Integrity	Availability	Security Class
60	STM Impedance Calculation Logs	Open Data	Low	Moderate	Moderate	1
64	Ridership: Fixed Route	Open Data	Low	Moderate	Moderate	1
65	Ride Gwinnett Complaint Log	Research	Moderate	Moderate	Moderate	2

2.4 Data Security Requirements

Table 4 provides a summary of data security requirements for each dataset based on the CIA assessment above. Safeguarding methods and processes which describe the method used to secure and gain access to data, have been identified. Those datasets that are designated as open have not been assigned safeguarding methods or procedures as they are not required to be secured. Combined datasets have been considered to ensure security is maintained. For example, users having a combination of datasets which by themselves do not need security but in combination do.

Table 4. Data Security Requirements

ID	Dataset Name	Access Level	Security Class	Safeguarding Methods and Processes
3	Whole Road Network	Open	1	NA
5	STM Network	Open	1	NA
8	OSM Network	Open	1	NA
10	Sidewalk Network	Open	1	NA
11	Indoor Pathways	Open	1	NA
15	NaviGAtor Data	Open	1	Although data is open, access to data is restricted by data usage agreement with GDOT. Third-parties typically must execute a user agreement with the data owner to access data.

ID	Dataset Name	Access Level	Security Class	Safeguarding Methods and Processes
20	Modeled Future Operating Conditions	Research / Proprietary	1	Access to licensed data may be granted by the data owner. Third-parties typically must execute a user agreement with the data owner to access data.
25	Network Impedance API	Operational; Open	1	NA
26	Roadway Design and Condition Data	Open	1	NA
27	Roadway Intersection Design and Condition Data	Open	1	NA
29	Pedestrian Intersection and Pathway Asset Design and Condition Data	Operational	3	NA
30	Building Pathway Asset Design and Condition Data	Open	1	NA
31	Building Wayfinding Asset Design and Condition Data	Open	1	NA
32	Transit Stop Asset Design and Condition Data	Open	1	NA
33	Transit Vehicle Asset Design and Condition Data	Operational	1	Access to licensed data may be granted by the data owner. Third-parties typically must execute a user agreement with the data owner to access data.
34	GTFS (Ride Gwinnett)	Open	1	NA
35	GTFS (MARTA)	Open	1	NA
36	GTFS Realtime (Ride Gwinnett)	Open	1	NA

ID	Dataset Name	Access Level	Security Class	Safeguarding Methods and Processes
37	GTFS Real-time (MARTA)	Open	1	NA
39	BSM	Operational	1	NA
44	Ped-X	Operational	1	NA
45	Trip options	Operational (real-time, transmitted, deleted), PII Certification (raw data)	4	Data protection governed by Georgia Tech secure sever systems data management protocols. Access conditions governed by NDA and approved IRB protocols.
46	VRU categories	Open	1	NA
51	Mobile App Logs	PII Certification (raw data); Open (when PII is removed)	3	Data protection governed by Georgia Institute of Technology (GA Tech) secure sever systems data management protocols. Access conditions governed by NDA and approved IRB protocols.
52	Traverse Data	PII Certification	3	Data protection governed by GA Tech secure sever systems data management protocols. Access conditions governed by NDA and approved IRB protocols.
53	Trip Feedback Reports	PII Certification (raw data); Open (when PII is removed)	3	Data protection governed by GA Tech secure sever systems data management protocols. Access conditions governed by NDA and approved IRB protocols.
58	ST-CTN Performance Measures Data	Open Data	1	NA
59	STM Communication Logs	Open Data	1	NA
60	STM Impedance Calculation Logs	Open Data	1	NA
64	Ridership: Fixed Route	Open Data	1	NA

ID	Dataset Name	Access Level	Security Class	Safeguarding Methods and Processes
65	Ride Gwinnett Complaint Log	Research	2	Data protection governed by GA Tech secure sever systems data management protocols. Access conditions governed by NDA and approved IRB protocols.

2.4.1 Relevant Privacy and/or Security Agreements

Formal privacy and security agreements are being developed among the stakeholder partners and data owners and will be executed prior to Phase 3. The [IPFP] describes the plan for generating these memoranda of understanding (MOU) and usage agreements among the stakeholder organizations operating and sourcing datasets. All dataset user and license agreements will be compiled when the system “goes live” and the team will make every effort to convince the data owners to make these datasets available in an open-source way that does not require the execution of a user agreement or payment of any fees. Several stakeholders (data owners) have already established data security, data privacy, and protected data access policies. The project dataset privacy and security agreements will incorporate appropriate agency dataset policy into these agreements.

The policies are described by the following columns:

- **Data Owner:** the owner and stakeholder responsible for issuing license or agreement.
- **Data Owner Type:** the type of organization issuing agreement or license. Values include: academic, public (public agency), commercial, and others.
- **Policy Type:** the type of policy or agreement issued by the data owner. Although the values vary by organization, the types of agreements contained in this table relate to dataset access, usage, security, and privacy.

Table 5. Relevant Privacy and Security Policies and Agreements

Data Owner	Data Owner Type	Policy Type	Policy Reference
ARC	Public	Data privacy and access policies	More details on the scope and type of policy and user agreements are included in the IPFP.
GA Tech	Academic	License and usage policies (copying, using, redistribution, etc.)	Usage Policy
GA Tech	Academic	Data privacy and access policies	Data access policy

Data Owner	Data Owner Type	Policy Type	Policy Reference
GA Tech	Academic	Data privacy and access policies	Data Privacy
GA Tech	Academic	Cybersecurity	Cybersecurity policy https://policylibrary.gatech.edu/information-technology/cyber-security-policy
GA Tech	Academic	Protected data practices	Protected data practices https://policylibrary.gatech.edu/information-technology/cyber-security-policy
GDOT - Smart Corridor Policies	Public	TBD, will be developed as part of the Connected Corridor project (Fall 2023)	TBD
SRTA/ ATL (for ATL RIDES)	Public	Network security policy	See [ATL DMP]
SRTA/ ATL (for ATL RIDES)	Public	Systems security policy	See [ATL DMP]

2.5 Risk Assessment of Threats

The ST-CTN project team recognizes that the use of data to support underserved communities inherently comes with risk; the thought of how to plan for and mitigate this risk has been considered throughout concept development (Phase 1) and during design and deployment (Phase 2).

Risk is assessed by considering the potential adverse effects caused by a particular threat or event and the likelihood of that event occurring – the impact and probability. The [NIST-2] recommends an assessment process in which the impact and probability of threats are analyzed to determine the potential risk severity and management approach.

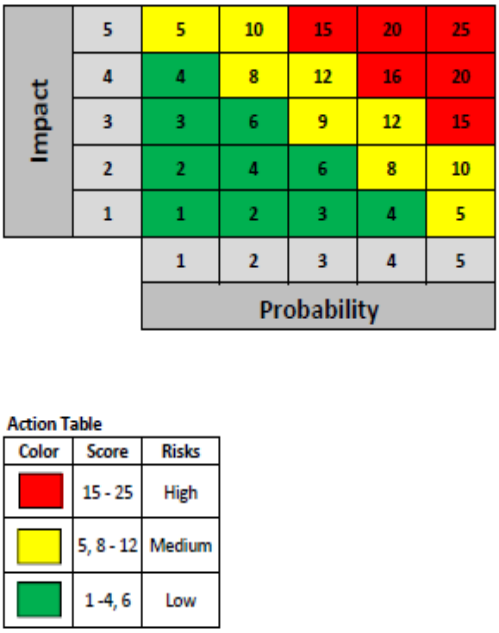
NIST defines a *threat source* as the exploitation of a vulnerability with intent and targeted method or a situation and method that may accidentally exploit a vulnerability. Types of threat sources include:

- hostile cyber or physical attacks;
- human errors of omission or commission;

- structural failures of organization-controlled resources (e.g., hardware, software, environmental controls); and
- natural and man-made disasters, accidents, and failures beyond the control of the project team.

The ST-CTN project team leveraged the CIA assessment in **Section 2.3.1** to identify those datasets with the highest security class. The potential threats associated with each dataset categorized as Class 3, 4, or 5 was considered more closely and assessed **Table 6** provides a summary of the assessment of threats for the ST-CTN project and includes the following fields:

- Threat Identification – brief description of the risk including potential schedule impacts.
- Associated Datasets – those datasets that would potentially be impacted if the identified threat event occurred.
- Impact – categorized as a number between 1 (very low) and 5 (very high) to indicate the scale of impact that would be caused by the risk.
- Probability – categorized as a number between 1 (very low) and 5 (very high) to indicate the likelihood of impact from the risk.
- Severity – product of the probability and impact (probability * impact) to describe the calculated risk. Severity ranges from 1 to 25 as shown in the Severity Matrix shown below.
- Risk Response – indicates the planned response to the risk; responses include: avoid, mitigate, accept, contingency, transfer.



Source: ARC, 2021

Figure 3. Risk Assessment Matrix

Table 6. Data Security Risk Assessment

Threat ID / Description	Associated Datasets	Impact	Probability	Severity	Risk Response
1 – Private Data Breach: Data at Rest Potential access breach in which an unauthorized person has access to data stored on STM data server.	51. Mobile App Logs 52. Traverse Data 53. Trip Feedback Reports 58. ST-CTN Performance Measures Data 59. STM Communication Logs 60. STM Impedance Calculation Logs	5	1	5	Avoid. This threat will be avoided by ensuring appropriate security controls are implemented including, managed physical access security, monitoring, encryption, use of a proxy server. Controls are further described in **Section 3**.
2 – Private Data Breach: Data in Transit Potential breach in which an unauthorized person accesses data in transit between the G-MAP secure server to STM data server.	51. Mobile App Logs 52. Traverse Data 53. Trip Feedback Reports 58. ST-CTN Performance Measures Data 59. STM Communication Logs 60. STM Impedance Calculation Logs	5	2	10	Avoid. This threat will be avoided by ensuring appropriate security controls are implemented including, monitoring, encryption, and use of a Virtual Private Network (VPN). Controls are further described in **Section 3**.

Threat ID / Description	Associated Datasets	Impact	Probability	Severity	Risk Response
3 – Private Data Breach: Data at Rest Potential access breach in which an unauthorized person has access to data stored on G-MAP third party secure server data server.	45. Trip Options (raw) 51. Mobile App Log (raw) 53. Trip Feedback Reports (raw)	5	1	5	Avoid. This threat will be avoided by the third-party secure server, MongoDB database hosted in AWS database service managed by AWS security controls which will used to store G-MAP private data.
4 – Private Data Breach: Data in Transit Potential breach in which an unauthorized person accesses data in transit between the G-MAP secure server to STM data server.	45. Trip Options (raw) 51. Mobile App Log (raw) 53. Trip Feedback Reports (raw)	5	2	10	Avoid. This threat will be avoided by ensuring appropriate security controls are implemented including, monitoring, encryption, and use of Internet Protocol (IP) whitelisting. Controls are further described in **Section 3**.

Threat ID / Description	Associated Datasets	Impact	Probability	Severity	Risk Response
5 – Ride Request Notification Breach It is possible that a RIDE Gwinnett transit rider may see a Ride Request notification intended for the transit operator which will indicate the stop where a G-MAP user is waiting and if they will need assistance boarding the vehicle.	Ride Request Dataset (External System)	2	2	4	Avoid. This threat will be avoided by including training to the RIDE Gwinnett operators to keep notifications of this sort private.

2.6 Data Sharing and Provision

The ST-CTN project team is making every effort to employ open access data to the greatest extent practicable in this project. The resulting transportation networks, sidewalk and roadway infrastructure design and condition data, and the STM will all be open access. With respect to agency data that traditionally require the execution of a data management agreement to ensure data integrity and track data usage, the team will execute agreements with the partners to allow the data to flow into the STM, at which time they become open access and can be accessed by the public.

Table 7 lists the current data license provisions for each of the datasets that are being employed in the project (data user agreement, data license agreement, and whether fees are currently associated with data use). Different open access license models may be applied to these datasets, depending upon the model that is currently being used and the data types within the dataset. At this point, the team has identified all current agency user agreements that must be executed to access agency data. However, as noted above, the project goal is to eliminate the need for these license agreements and to make the agency data available through the open access Public PMD.

The columns in **Table 7** include:

- **Dataset Owner:** owner of the dataset.
- **Dataset ID(s) and Dataset Title(s):** group of datasets that are subject to the same license.
- **Access Level:** describes how individuals may gain access or how the datasets may be used. Values include: PII Certified, Research, Proprietary, Operational and Open.
- **License Used**: the license applied to the dataset(s).
- **Reasons for a Non-Open License**: the reason why no license is applied or a non-open license is used for a dataset.

Table 7. Data Owner License Applied to Datasets

Data Owner	Dataset IDs and Titles	Access Level	License Used	Reason(s) for Non-Open License
ARC	3. Whole Road Network 10. Sidewalk Network 11. Indoor Pathways 46. VRU categories	Open	TBD	N/A
ARC	51. Mobile App Logs (raw) 53. Trip Feedback Reports (raw)	PII Certification	See Phase 2 DMP and requires IRB Protocol Approval	Protection of PII

Data Owner	Dataset IDs and Titles	Access Level	License Used	Reason(s) for Non-Open License
ARC	51. Mobile App Logs (removed PII)	Research	Will be covered by usage agreement	Contains trace data but may be used for research purposes.
ARC	53. Trip Feedback Reports (removed PII)	Open	Will be covered by usage agreement	Contains trace data but may be used for research purposes.
ARC	45. Trip options	Operational (realtime, transmitted, deleted), PII Certification (raw data)	IRB Protocol Approval	Protection of PII. The turn-by-turn data reveal home and work locations and constitutes PII. Even subsets of data that occur repeatedly, such as travel distance, reveal home location.
ARC / GA Tech	58. ST-CTN Performance Measures Data	Open	N/A	N/A
ARC / GA Tech	59. STM Communications Logs 60. STM Impedance Calculation Logs	Open	TBD	N/A
ARC / GCDOT	44. PED-X	Operational	TBD	N/A
Facility owner	30. Building Pathway Asset Design and Condition Data 31. Building Wayfinding Asset Design and Condition Data	Open	TBD	N/A

Data Owner	Dataset IDs and Titles	Access Level	License Used	Reason(s) for Non-Open License
GA Tech	52. Traverse Data	PII Certification	IRB Protocol Approval	Protection of PII
Ride Gwinnett	33. Transit Vehicle Asset Design and Condition Data	Operational	TBD	N/A
Ride Gwinnett	34. GTFS (Ride Gwinnett) 36 GTFS Realtime (Ride Gwinnett) 64. Ridership: Fixed Route	Open	TBD	N/A
Ride Gwinnett	65. Ride Gwinnett Complaint Log	Research	IRB Protocol Approval	Protection of PII
GDOT	15. NaviGAtor Data	Open	GDOT User Agreement	User agreement ensures data integrity, tracks data use, and facilitates secure data access
GCDOT	39. BSM	Operational	License and usage agreements will be developed as part of the Connected Corridor Project	N/A
Gwinnett County	29. Pedestrian Intersection and Pathway Asset Design and Condition Data	Operational	TBD	N/A
Gwinnett County	32. Transit Stop Asset Design and Condition Data	Open	TBD	N/A
MARTA	35. GTFS (MARTA) 37. GTFS Real-time (MARTA)	Open	MARTA (itsmarta.com)	N/A
OSM	8. OSM Network	Open	CC BY-SA 2.0	N/A

Data Owner	Dataset IDs and Titles	Access Level	License Used	Reason(s) for Non-Open License
STM	20. Modeled Future Operating Conditions	Research / Proprietary	License agreements executed with owners of models or individual model scenario runs.	User agreement ensures data integrity, tracks data use, and facilitates secure data access.

2.7 Specific System Hardware Security Analysis

This section provides a summary of all key system hardware components and references any security concerns.

2.7.1 Component 1 – GA Tech Secure Compute Server

The secure compute server consists of a 1U rack mounted server with 96 compute cores. The unit resides in a server equipment room in the GT Sustainable Education Building (SEB). The Internal Security Group personnel are the only employees with access to this room. The server is connected to the Secure Data Lab over a network that is installed behind an additional firewall that separates the network from the rest of the building's network. Employees with clearance to access the PII data can access the server by connecting from specific designated terminals in the Secure Data Lab. The PII data is received by the compute server and is stored on the secure storage server. Any processing of the data, including the processes for anonymization of the PII data occurs on this compute server. Performance measures data will be analyzed, anonymized, and shared with the open access Public PMD and is described further in the Phase 2 DMP. There are minimal security concerns related to any unauthorized access due to the extensive physical security of the server.

2.7.2 Component 2 – GA Tech Secure Storage Server

The secure storage server consists of a 2U rack mounted server with 140 TB of storage. The storage server is located in the same server equipment room as the compute server and is connected to the same secure network. The PII data as well as the anonymized data are stored on this server before parts of the anonymized data are pushed out to the STM. There are minimal security concerns related to any unauthorized access due to the extensive physical security of the server.

3 Security Controls

This section describes the technical and policy controls used to provide data security for the ST-CTN system, as well as the plan of action that will be taken in the case of a data breach.

3.1 Technical Controls

Technical controls related to protecting and securing ST-CTN private data are described in the following subsections.

3.1.1 Access

Access to raw data is stored and archived to ensure data integrity. Data used in active implementation of the system will appear in online working datasets that are updated and queried in realtime. PII data protection is governed by GA Tech secure server systems data management protocols which include the following:

- Elimination of remote access to the Secure Server.
- Direct hard-wire connections between the Secure Server and the data analysis terminals which are located in the Secure Data Lab in the Sustainable Education Building (SEB).
- Secure Data Lab door security that requires cardkey access.

Access to protected data is governed by non-disclosure agreement (NDA) and approved IRB protocols:

- IRB approval is required for any access to PII data (amendments may be submitted to facilitate supplemental data access and uses while ensuring continued privacy protection).
- Individual access to the data requires card key access to the Secure Data Lab, login ID and password access to the Secure Data Lab terminals, and pre-approved login ID and password access to the secure server, login ID and password access to each data folder.
- Access to PII data can only be accomplished through dedicated direct-connect terminals located in the Secure Data Lab in the Sustainable Education Building (no remote access).

3.1.2 Logging and Monitoring

Technical controls will include logging and monitoring for unexpected access or suspicious activity. Protected data is only accessible with:

- Login ID and password protection to terminals and the secure server.
- Layered protection within the secure server data storage system to limit access to different datasets to specific users.

3.1.3 Encryption

PII data protection is governed by GA Tech secure sever systems data management protocols which include the following encryption related controls:

- Transmission of encrypted PII data to the GA Tech interface server.
- Decryption of data on the GA Tech Secure Server.

3.2 Policy Controls

Policy controls related to protecting and securing ST-CTN private data are described in the following subsections. Policy controls will be governed by the IRB and Enterprise Data Governance (EDG) Data Committee. The EDG will establish governance for integrated datasets and is described further in the Phase 2 DMP. It should be noted that the EDG will remain consistent with all IRB protocols and policy controls.

It should be noted that state and local policies are not included herein but can be found in the Privacy Management Plan (PrMP) which is not a deliverable to the USDOT. However, the ST-CTN project team will confirm their intent to follow state and local policies through a signed statement to the USDOT.

3.2.1 Cybersecurity Policies

Similar to privacy and security policies, each organization hosting or managing a datastore will drive the cybersecurity policies for their datasets. A set of agreements on the overall security processes to be put in place will be developed as part of the EDG committees described earlier in this section.

The policies are described by the following columns:

- **Data Owner:** the owner and stakeholder responsible for the policy.
- **Data Owner Type:** the type of organization issuing policy. Values include academic, public (public agency), commercial, or other.
- **Policy Type:** the type of policy issued by the data owner. The values may include network, system and cybersecurity policies and procedures.
- **Policy Reference:** a link or reference to the policy provisions.

Table 8. Cybersecurity Policies and Procedures

Data Owner	Data Owner Type	Policy Type	Policy Reference
SRTA/ATL	Public	Network security policy	[ATL DMP]
SRTA/ATL	Public	System security policy	[ATL DMP]
GDOT	Public	Connected Corridor Security and IT Policies (TBD)	TBD
GA Tech	Academic	Security Procedures and Standards	Cyber-security-policy https://policylibrary.gatech.edu/information-technology/cyber-security-policy

3.2.2 Back-up and Recovery Policies and Procedures

Similar to privacy and security policies, each organization hosting or managing a datastore will implement existing policies and procedures for back-up and recovery. A set of agreements on the overall retention and recovery processes to be put in place will be developed as part of the EDG committees described earlier in this section.

The current individual dataset owner policies are described by the following columns:

- **Data Owner:** the owner and stakeholder responsible for the policy.
- **Data Owner Type:** the type of organization issuing policy. Values include academic, public (public agency), commercial, or other.
- **Policy Reference:** a link or reference to the policy provisions.

Table 9. Data Archiving and Retention Policies and Procedures

Data Owner	Data Owner Type	Policy Reference
SRTA/ ATL	Public	[ATL DMP]
GA Tech	Academic	Data Archiving and Retention Policy https://gatech.service-now.com/technology?id=kb_article_view&sysparm_article=KB0022866

3.2.3 Breach Plan

This section summarizes the action plan the ST-CTN project team will take should there be a breach in data security. Responding to data security breaches in an effective, timely manner will minimize potential impacts and severity of those impacts to the project, while limiting project risk exposure. The first step in managing a breach in data security is to identify, monitor, and manage risk.

Each risk associated with a potential breach in data security will be identified and considered by the Executive Management Team (EMT) and risk owner (if outside of the EMT). In addition, risks will continue to be identified and monitored throughout development, deployment, and operations.

Depending on the significance of the risk, the EMT will determine if the risk needs to be documented within the ST-CTN Risk Registry. If the risk is of significance, risk responses will be planned and documented within the ST-CTN Risk Registry.

Consistent with the Project Management Body of Knowledge (PMBOK) Guide, risk responses will be categorized as follows:

- Avoid – Eliminate the threat or condition or to protect the project objectives from its impact by eliminating the cause.
- Mitigate – Identify ways to reduce the probability or the impact of the risk.
- Accept – Nothing will be done.
- Contingency – Define actions to be taken in response to risks.
- Transfer – Shift the consequence of a risk to a third-party together with ownership of the response by making another party responsible for the risk (buy insurance, outsourcing, etc.).

For each risk subject to response planning, the responsible Co-Project Management Lead (Co-PML), in collaboration with project team members responsible for activities potentially impacted by the risk if triggered, will be tasked with identifying ways to prevent the risk from occurring or reduce its probability of occurring.

In the event that the risk is not successfully managed and a breach in data security occurs, the following steps will be taken:

Step 1 – The EMT is notified immediately by the team member who has recognized the breach (or potential breach).

Step 2 – The EMT will coordinate with the technical lead most knowledgeable about the event.

Step 3 – Together, the EMT and technical lead will determine how the breach can be isolated or contained.

Step 4 – EMT will determine the risk to End Users and how they will be notified if necessary. Determine any laws that need to be adhered to and share that information with the technical lead.

Step 5 – After the risk and nature of the breach is determined, the EMT will notify the USDOT of any breach critical in nature. The USDOT will be notified of any breach that requires End Users to be notified or that have the potential to impact performance measures.

Step 6 – The technical lead will update the EMT regularly. For those breaches which are of critical nature, the technical lead will update the EMT every three hours to provide resolution status, causation findings, damage, and expected resolution time.

Step 7 – Upon breach resolution, the EMT will conduct an after-action meeting with the ST-CTN project team to review the cause of the breach, resolution, and analysis of how the breach was handled. The project team will consider how to ensure a similar event does not occur and any opportunities for improvement or lessons learned.

Appendix A. Acronyms and Glossary

This section provides acronyms, abbreviations, and glossary of terms used throughout the DPP.

Acronyms

ABM - Activity Based Model

API – application programming interface

ARC – Atlanta Regional Commission

ATIS – Advanced Traveler Information System

ATL – Atlanta-Region Transit Link Authority

ATL RIDES – Atlanta-Region Rider Information and Data Evaluation System

BSM – basic safety message

CDP – Connected Data Platform

ConOps – Concept of Operations

CV – connected vehicle

CV1K – Regional Connected Vehicle Infrastructure Deployment Program

C-V2X – Cellular – Vehicle to Everything

CVTMP – Connected Vehicle Technology Master Plan

DSRC – Dedicated Short-Range Communication

DMP – Data Management Plan

DOR – Department of Revenue

DPP – Data Privacy Plan

FHWA – Federal Highway Administration

FTA – Federal Transit Administration

G-MAP – Georgia Mobility and Accessibility Planner

GA Tech – Georgia Institute of Technology

GDOT – Georgia Department of Transportation

GTFS – General Transit Feed Specification

GTRI – Georgia Tech Research Institute

ICD – interface control document

IE – independent evaluator

IOO – infrastructure owner and operator

IRB – Institutional Review Board

ITS – Intelligent Transportation Systems

JPO – Joint Program Office

JSON – JavaScript Object Notation

KPI -- key performance indicators

LEP – limited English proficiency

MAP – MapData

MARTA – Metropolitan Atlanta Rapid Transit Authority

MOU – memoranda of understanding

MOVES – motor vehicle emissions simulator

MU – mobile unit

MVP – Minimum Viable Project

NDA – non-disclosure agreement

NOAA - National Oceanic and Atmospheric Administration

OBU – onboard unit

OSM – OpenStreetMap

OSS – Open Source Software

OST – Office of the Secretary

OTP – Open Trip Planner

PACE – Partnership for an Advanced Computing Environment

PED-SIG – Mobile Accessible Pedestrian Signal System

PICS – protocol interface conformance specification

PII – personally identifiable information

PMBOK – Project Management Body of Knowledge

PMD – Performance Management Dashboard

PROW – public right of way

PSM – pedestrian safety message

REST – representational state transfer

ROW - right of way

RSU – roadside unit

SPaT – signal phasing and timing

SRM – signal request message

SRTA - State Road and Tollway Authority

SSM – signal status message

ST-CTN – Safe Trips in a Connected Transportation Network

STM – space time memory

TBD – To Be Determined

TMC – traffic management center

TPI – transit pedestrian indication

TSP – transit signal priority

TSR – transit stop request

USDOT – U.S. Department of Transportation

VRU – vulnerable road user

WZDX - Work Zone Data Exchange

XML – extensive markup language

The following table provides a summary of terms by category used throughout the DPP.

Table 10. Glossary

Category	Term	Definition
Dataset Type	Assets	Asset information about facility and ATMS devices-- sensors, signals, comm including electronic signs, PED-X signals, etc.
Dataset Type	Crowdsource	Data generated by the "crowd"
Dataset Type	CV	Connected vehicle produced dataset
Dataset Type	Demographics	Data about the structure of populations
Dataset Type	Land Use	Human use of land
Dataset Type	Mobility Service API	Application programming interfaces (API) or services that are pushed or pulled by an application.
Dataset Type	Network	Infrastructure characteristics and topological connectivity including right of way, PROW (sidewalk, crosswalk, bike lanes/paths)
Dataset Type	Network operating conditions	Condition and status of network infrastructure including planned and unplanned events: incidents, special events, work zones, and other impacts.
Dataset Type	System-Customer Performance	Data sets that require archiving and use by performance measures
Dataset Type	Transit	Transit network (routes) and realtime conditions/event data
Dataset Type	VRU Modes	Types of VRUs; used to describe categories of default impedance values
Dataset Type	Weather	Weather data

Category	Term	Definition
Access Level	PII Certification	Data that has PII included in the data set. The access to this data should be as restrictive as possible to protect the PII based on IRB-approved processes. Data in this category should have an operational purpose that justifies its storage.
Access Level	Private	Data that cannot be shared with external users. Access to these data is limited and only granted with IRB and Project Team approvals. Private data include four subcategories: operational, proprietary, research and PII Certification.
Access Level	Proprietary	Licensed data from third parties or CBIs. This data may be used for planning or operational purposes. Any access to the data is determined by usage agreements between the parties.
Access Level	Operational	Realtime and other data used in the applications and operations of the system. The data may contain licensed data restricted by usage agreements.
Access Level	Research	Data that is available for research, but users of the data must meet IRB requirements before gaining access to the data. These datasets may have PII. These datasets are compiled for machine learning and research purposes that do not contain PII.
Access Level	Open	Data that can be used by the public with no or limited licensing restrictions. This data is available to the public without needing to request permissions and will be provided to the USDOT-managed Public System. These will be anonymized or aggregated version of private datasets to protect PII.
Collection Method	Derived	Data is derived from one or more sources for summary or fusion purposes
Collection Method	External Input	Data is ingested from a third party source (the ingestion process may be through a digital interface or through manual processes.)
Collection Method	Collect / forward	Data created, collected, forwarded and stored. These include user input transactions (e.g., between APIs), web forms, user tracking methods (e.g., trace data from mobile phones)

Appendix B. References

This section includes a list of documents referenced during the plan, including URLs and USDOT Publication Numbers, where possible.

ID	Referenced Documents
[ConOps]	Atlanta Regional Commission. Deliverable Task 2 Concept of Operations. Atlanta: U.S. Department of Transportation. (2021).
[CV1K]	Georgia Department of Transportation. "The Regional Connected Vehicle Program Scope of Work." Atlanta: Georgia Department of Transportation.
[CVTMP]	AECOM. "Gwinnett County Connected Vehicle Technology Master Plan (CVTMP)." Duluth: Gwinnett County Department of Transportation. (2019).
[DMP]	Atlanta Regional Commission. Deliverable Task 3 Data Management Plan. Atlanta: U.S. Department of Transportation. (2021).
[GTFS]	GTFS. General Transit Feed Specification Reference. Washington D.C.: GTFS. (2019).
[ICD]	Georgia Department of Transportation. Deliverable Task 2B Interface Control Document. Atlanta: U.S. Department of Transportation. (2023).
[IPFP]	Atlanta Regional Commission. Deliverable Task 10 Institutional, Partnership, and Financial Plan. Atlanta: U.S. Department of Transportation. (2022).
[NIST-1]	National Institute of Standards and Technology. (2004). *Standards for Security Categorization of Federal Information and Information Systems.* Federal Information Processing Standards (FIBS) Publication 199.
[NIST-2]	National Institute of Standards and Technology. (2012). *Guide for Conducting Risk Assessments.* National Institute of Standards and Technology.
[NIST-3]	Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *An Introduction to Information Security (NIST Special Publication 800-12).* National Institute of Standards and Technology.
[PMBOK]	Project Management Institute. (2017). *Project Management Body of Knowledge, 6th Edition*
[PMESP]	Atlanta Regional Commission. Deliverable Task 5 Performance Measurement and Evaluation Support Plan. Atlanta: U.S. Department of Transportation. (2021).

[SySR]	Atlanta Regional Commission. Deliverable Task 6 System Requirements Specification. Atlanta: U.S. Department of Transportation. (2021).
[USDOT-1]	USDOT. (2023, 06 19). *Device Classes*. Retrieved from ARC-IT Version 9.1 The National ITS Reference Architecture: https://www.arc-it.net/html/security/deviceclasses.html
[USDOT-2]	USDOT. (2023, 06 19). *Security.* Retrieved from ARC-IT Version 9.1 The National ITS Reference Architecture: https://www.arc-it.net/html/security/security.html
[VPFP]	Guensler, R., Y. Xu, V. Elango. Value Pricing Fellowship Project. Atlanta: Georgia Department of Transportation. (2013).

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-22-970

U.S. Department of Transportation