Data Privacy Plan

for the Smart Columbus Demonstration Program

FINAL REPORT | November 7, 2019

ANNUAL UPDATE | September 24, 2020

Produced by City of Columbus

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

Acknowledgement of Support

This material is based upon work supported by the U.S. Department of Transportation under Agreement No. DTFH6116H00013.

Disclaimer

Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the Author(s) and do not necessarily reflect the view of the U.S. Department of Transportation.

Acknowledgements

The Smart Columbus Program would like to thank the following members for their support of Smart Columbus and their work on the Technical Working Group Policy Team.

Dennis Hirsch, The Ohio State University	Mehmet Munur, Tsibouris & Associates
Kirk Herath, Nationwide Insurance	Dorene Stupski, Marriott International
Keir Lamont, The Ohio State University	Charles Campisano, City of Columbus
Tom Harris, HMB	Ty Sonagere, CoverMyMeds
Daren Arnold, State of Ohio	Doug McCollough, City of Dublin
David Landsbergen, The Ohio State University	Amanda Girth, The Ohio State University
David Daniel, Nationwide Insurance	Jeff Hunsaker, HMB
Jeff Kanel, Centric	John Sohner, HMB
Nick Nigro, Atlas Policy	Brian Nutwell, Honda
Jim Perry, CAS	Jack Maher
Peter Voderberg, State of Ohio	Christina Drummond, The Ohio State University
Schlaine Hutchins, CoverMyMeds	

The Smart Columbus Program would also like to thank the authors, reviewers, and contributors to this Data Privacy Plan.

Mandy Bishop, City of Columbus	Andrew Wolpert, City of Columbus
Jodie Bare, City of Columbus	Ryan Bollo, City of Columbus
Tammy Chellis, Accenture	Sherry Kish, HNTB
Brian King, Proteon	Victor Blue, HNTB
Warner Moore, Gamma Force	Ram Boyapati, Battelle
Mihail Chirita, Agile Answers	Jeff Kupko, Michael Baker International

Abstract

The Smart Columbus Demonstration Program Data Privacy Plan (DPP) provides an overarching framework for the ways in which Smart Columbus will protect the security of personal information that it collects and uses, and the privacy of the individuals to whom this information pertains. Smart Columbus is committed to be a responsible steward of this personal information. The DPP makes clear this commitment in its Statement of Data Stewardship Principles (Chapter 3). It then defines controls for data privacy (Chapter 4) and data security (Chapter 5). Together, these components provide a structure for protecting data throughout the Smart Columbus Operating System.

In addition to this DPP, system security protocols for non-PII data are contained in project-specific documents.

Table of Contents

List of Tables

List of Figures

Executive Summary

This Data Privacy Plan (DPP) provides high-level guidance, principles, and policies to ensure the privacy of Smart Columbus Demonstration data subjects and project participants. While the City of Columbus Smart Columbus Program Office oversees many innovation initiatives, the scope of this document includes all data in the Smart Columbus Operating System (Operating System) and other United States Department of Transportation (USDOT) funded projects. The City of Columbus USDOT-funded Smart Columbus program will be known throughout this document as Smart Columbus.

The intended audience includes the Smart Columbus project managers, the USDOT, transportation researchers, the Institutional Review Board (IRB), and those engaged in the deployment of Smart Columbus projects.

This document applies to all individuals who use or share data with Smart Columbus, including all Smart Columbus employees, partners, and consultants. Where applicable, contract and other acquisition-related documents will include terms providing for compliance with the requirements of this DPP.

SCOPE AND APPROACH

To provide more efficient, equitable, and sustainable transportation options, Smart Columbus needs to collect and process certain categories of personal information. Smart Columbus is committed to good stewardship of this personal data, providing notice and consent for collecting personal information, collecting the minimum amount of personal information necessary to achieve its specified purposes, protecting it securely, and handling it with respect for individual privacy and autonomy. This DPP sets out the measures that Smart Columbus is taking to ensure the privacy of demonstration data subjects and participants in Smart Columbus projects.

This DPP describes the principles that guide the Smart Columbus project teams in developing governance documents to protect the privacy of users and participants, guard against potential breaches of Smart Columbus systems, and prevent unauthorized use of the participant data and other Personally Identifiable Information (PII). Therefore, the DPP informs all contracts, notices, and processes that are being formed to comply with its stated approach to security and privacy for the Operating System and all Smart Columbus projects. Any successor entity to the City of Columbus shall comply with this DPP with respect to the data collected under the policy.

This DPP sets out high-level privacy protections and oversight governing Smart Columbus. The initial plan was developed early in the Smart Columbus program and set forth the system essentials to which project-level clarifications have been added quarterly, as Smart Columbus projects progressed. The approach to documenting high-level privacy protections and oversight has been iterative, bringing this high-level plan forward in manageable steps as the projects that it guides have informed it. The DPP's overarching controls are the layered lines of defense for this program. While this plan discusses each control being undertaken, four of these are considered the program's main protections: IRB, Privacy Impact Assessment, de-identification, and data curation. Each of these are discussed below.

Project-level data privacy development used the guidance of this plan to resolve project-level designs. Details of data privacy for data subjects are realized as part of the systems engineering process as user needs and requirements are developed under IRB oversight.

The treatment of project participants and their PII has been and will be defined by IRB processes that are consistent with this DPP, made through IRB-approved informed consent documents and research protocol documents.

The Data Management Plan for the Smart Columbus Demonstration Program (DMP) is a companion document to this DPP, and describes how data will be collected, managed, integrated and disseminated before, during, and after the Smart City Challenge demonstration. This DPP provides privacy and security guidelines and controls that govern Smart Columbus and, therefore, is the highest-level governing reference for the projects in this program. It does not address system security of the individual demonstration projects. The requirements for each individual project will separately address system security.

Chapter 1. Introduction

1.1. PROJECT DESCRIPTION

In 2016, the U.S. Department of Transportation (USDOT) awarded $40 million to the City of Columbus, Ohio, as the winner of the Smart City Challenge. With this funding, Columbus is addressing the most pressing community-centric transportation problems by integrating an ecosystem of advanced and innovative technologies, applications, and services to bridge the sociotechnical gap and meet the needs of residents of all ages and abilities.

With the award, the City established a strategic Smart Columbus program with the following vision and mission:

- **Smart Columbus Vision:** Empower residents to live their best lives through responsive, innovative, and safe mobility solutions.
- **Smart Columbus Mission:** Demonstrate how Intelligent Transportation Systems (ITS) and equitable access to transportation can have positive impacts on every day challenges faced by cities.

While the City of Columbus Smart Columbus Program Office oversees many innovation initiatives, the scope of this document is any data that is in the Operating System or that is in any of the other USDOT-funded projects. The City of Columbus USDOT-funded Smart Columbus program is known throughout this document as Smart Columbus.

To enable these new capabilities, the Smart Columbus program is organized into three focus areas addressing unique user needs: enabling technologies, emerging technologies, and enhanced human services. The individual projects described below were categorized into these three focus areas as seen in **Figure 1**: Smart Columbus Framework.

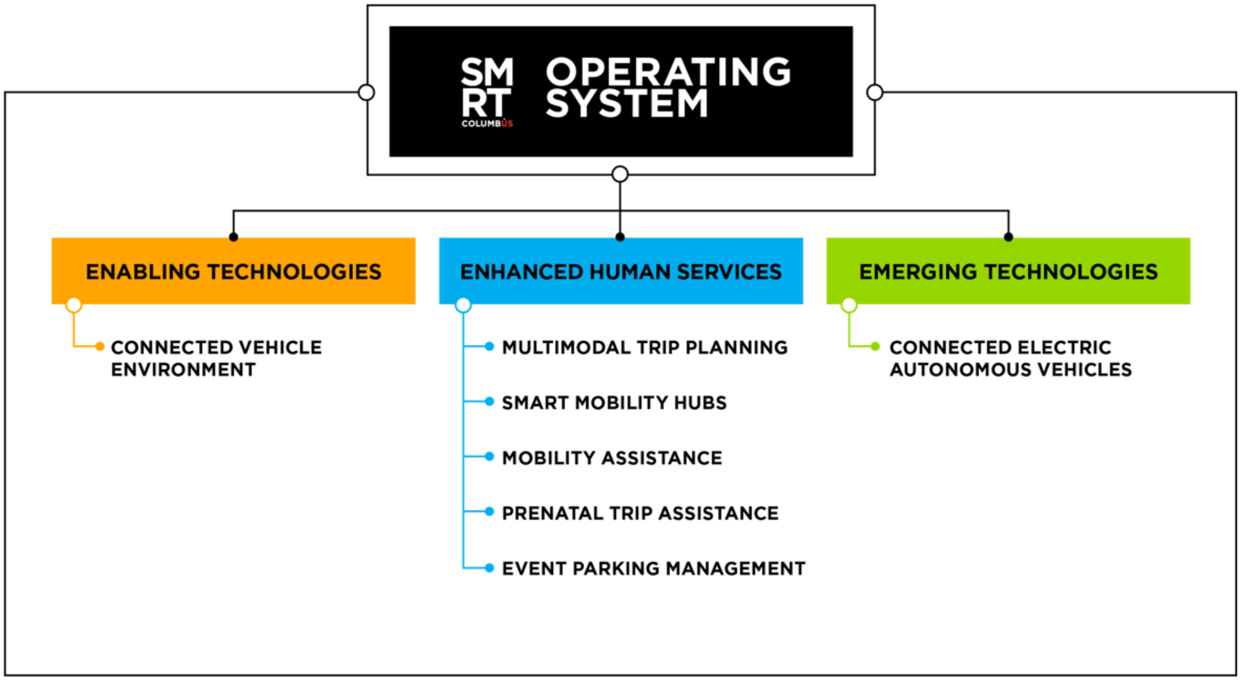


Figure 1: Smart Columbus Framework

Source: City of Columbus

The Columbus Smart City Demonstration Projects include the following:

- **The Smart Columbus Operating System (Operating System)**

  The Operating System is the essence of Smart Columbus—it brings to life the innovation. The Operating System is designed and built to collect data from a variety of inputs, including public, nonprofit, education-based, and private-sector contributors. These inputs may come from other systems, devices, and people—all of which are a critical part of building this ecosystem of innovation. Data is available for analytics and visualization. The Operating System is a platform designed for Big Data, Machine Learning and Artificial Intelligence, Analytics, and complex data exchange. It captures data and provides a means for multitenant access to aggregate, fuse, and consume data.

  Datasets housed in the Operating System include the Smart Columbus demonstration projects, traditional transportation data, and data from other community partners, such as food pantries and medical services. The Operating System is scalable and demonstrates the potential for serving city and private sector needs well beyond the life of the Smart City Challenge award period.

- **Connected Vehicle Environment (CVE)**

  Cars, trucks, and buses will talk to the infrastructure and talk to one another to reduce traffic congestion and increase safety. The CVE will connect up to 1,200 vehicles and over 90 smart intersections across the region. Safety applications are intended to be installed on multiple vehicle types including transit buses, first responder vehicles, city and partner fleet vehicles, and private vehicles. Applications will be deployed to ensure emergency vehicles and the Central

Ohio Transit Agency (COTA) Bus Rapid Transit (BRT) fleet can utilize signal prioritization when needed to ensure safety and efficiency.

- **Multimodal Trip Planning Application (MMTPA)**

  The MMTPA provides a robust set of transit and alternative transportation options—including routes, schedules, and dispatching possibilities. The application, named Pivot, allows travelers to request and view multiple trip itineraries and make reservations for shared-use transportation options such as bike-sharing, ride-hailing, and scooter-sharing. Users will be able to compare travel options across modes, and plan and pay for their travel based upon current traffic conditions and availability of services.

- **Smart Mobility Hubs (SMH)**

  Smart Mobility Hubs were deployed to serve traveler needs more effectively by expanding transportation resources and offering access to comprehensive trip planning tools at designated locations. SMH sites are primarily located adjacent to existing COTA CMAX and transit center facilities and help bridge the first mile/last mile gap between transit and destination by providing physical space for the consolidation of services such as bike-/scooter-share, car-share, and ride-hailing. Interactive kiosks and public Wi-Fi are available to the traveler to view real-time travel information and to book multimodal trip plans via the Pivot app.

- **Mobility Assistance for People with Cognitive Disabilities (MAPCD)**

  The City deployed an innovative smartphone application for people with cognitive disabilities to transition away from costly paratransit services and increase independent travel on the fixed-route bus system. The application was piloted with 20 individuals in the Columbus region in partnership with COTA and The Ohio State University (OSU). The application included a highly accurate, turn-by-turn navigator designed to be sufficiently intuitive such that older adults and groups with disabilities, including the cognitively disabled, could travel independently.

- **Prenatal Trip Assistance (PTA)**

  The City developed a system for providing flexible, reliable, two-way transportation to expectant mothers through a smartphone application, website, and call center. The project uses Medicaid Managed Care Organization brokered, non-emergency medical transportation services who are HIPAA compliant.

- **Event Parking Management (EPM)**

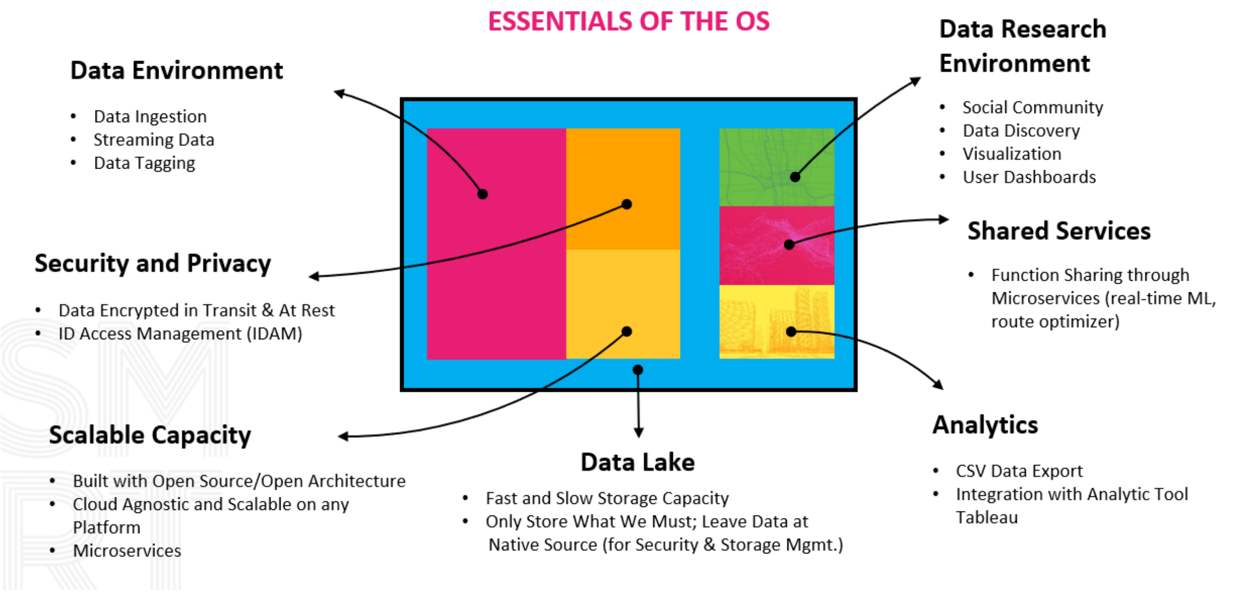
  The EPM system will integrate parking information from existing garages, surface lots, and parking meters in Downtown and the Short North into a single mobile application and web-based solution. This system will allow travelers to search for and reserve parking in advance or on the go. More direct routing of travelers during large events is expected to reduce congestion.

- **Connected Electric Autonomous Vehicles (CEAVs)**

  CEAVs that operate in a mixed-traffic environment interacting with other vehicles, bicyclists, and pedestrians have been deployed. The project provides an accessible and easily expandable first mile/last mile transportation solution to the region by deploying a fleet of multi-passenger CEAVs that leverage the enhanced connectivity provided by the CVE and the citywide travel-planning solution.

1.2. CORE FUNCTIONS OF THE OPERATING SYSTEM

Figure 2: Core Functions of the Smart Columbus Operating System depicts high-level system elements of the Operating System.



ESSENTIALS OF THE OS

Data Environment

- Data Ingestion
- Streaming Data
- Data Tagging

Security and Privacy

- Data Encrypted in Transit & At Rest
- ID Access Management (IDAM)

Scalable Capacity

- Built with Open Source/Open Architecture
- Cloud Agnostic and Scalable on any Platform
- Microservices

Data Lake

- Fast and Slow Storage Capacity
- Only Store What We Must; Leave Data at Native Source (for Security & Storage Mgmt.)

Data Research Environment

- Social Community
- Data Discovery
- Visualization
- User Dashboards

Shared Services

- Function Sharing through Microservices (real-time ML, route optimizer)

Analytics

- CSV Data Export
- Integration with Analytic Tool Tableau

Figure 2: Core Functions of the Smart Columbus Operating System

Source: City of Columbus

The Operating System is a platform for smart cities' development and operation. It consists of several core functions, which can be leveraged across the Smart Columbus program, as well as other functions (defined below) that will specifically enhance and support the "Smart Applications." The Operating System has the following core functions:

- **Data Environment:** The orderly ingestion and tagging of many forms of data from real-time, to slow-moving, or manually uploaded data.
- **Data Lake:** A storage repository that holds a massive amount of raw data in a secure way and makes it available to all other supported operations in the system.
- **Security and Privacy:** To ensure trust, it is imperative that the Operating System manages the users and systems that have access to it.
- **Scalable Capacity:** The Operating System is "scalable" and "elastic," which means that it can grow and shrink to meet the demand of the system at any given time.
- **Shared Services Environment:** Application components can be housed and made available to any number of applications connected to the Operating System.
- **Data Research Environment:** Agencies will be supported with user dashboards and visualizations to help improve their data-driven decision making.

- **Analytics:** The ability to query and combine datasets made available through Application Programming Interfaces (APIs), visualization tools within the Operating System, and integrating with tools external to the Operating System.

1.3. SYSTEM OF SYSTEMS OVERVIEW

The Smart Columbus program has many interrelated systems that work together to provide a System of Systems (SoS). Information from these systems is shared in the Smart Columbus Operating System. Both real-time and archived data are maintained in the Operating System for use by other Smart Columbus projects and future applications. The SoS provides Smart Applications, Smart Vehicles, and Smart Infrastructure to travelers in the Columbus area. The Operating System enables the SoS to share data with many other external systems to provide the framework for the services provided. **Figure 3**: System of Systems External Context Diagram shows the relationship of the SoS to the external travelers and systems.

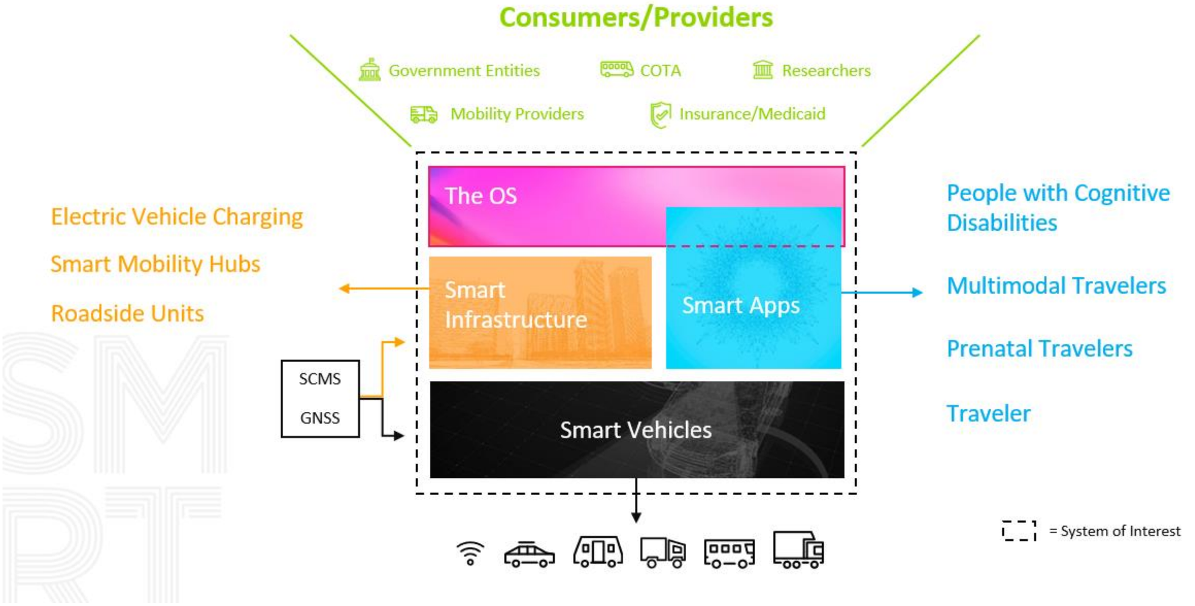


Figure 3: System of Systems External Context Diagram

Source: City of Columbus

The Smart Infrastructure element contains the roadside units (RSUs), hubs, and corresponding network that enable interactions between these items and the Operating System. Smart Vehicles include the onboard units (OBUs) that will be installed in vehicles and include various vehicle types. Smart Applications include the software-oriented solutions that will deliver other Smart Columbus project capabilities such as multimodal trip planning and prenatal trip assistance. The Operating System is the repository for all performance data from the Smart Infrastructure and Smart Vehicles.

1.4. TRANSPARENCY AND PUBLIC ENGAGEMENT

The Smart Columbus team maintains two public websites. The first, www.smart.columbus.gov, has current information about all Smart Columbus projects. Current information can include system engineering documentation for each project, opportunities to get involved in Smart Columbus, project webinars, and topical knowledge sharing.

The second website, www.smartcolumbusos.com, is the Operating System which includes open data (including project, public, nonprofit, education-based, and private-sector data), educational material regarding using and sharing data in the portal, and all policies and procedures for Operating System operation and information about the datasets on the Operating System.

The City shall include a mechanism for the public to give feedback on both websites. On the Operating System website, users will also be able to assess the quality of published information, provide input about what information should be a priority for inclusion, and provide overall input on the Operating System.

Another layer of public engagement that is afforded to Smart Columbus through USDOT is to add project datasets to the USDOT JPO ITS DataHub at www.its.dot.gov/data. The Smart Columbus datasets can be found by typing “Smart Columbus” into the search bar.

1.5. ROLES

Smart Columbus will appoint individuals with the following roles:

- Chief Privacy Officer – Responsible for the sustained viability, compliance, and oversight of data privacy policies and processes.
- Chief Security Officer – Responsible for the design, implementation and oversight of the information technology and physical security of the program and its project components.
- System Administrators – Responsible for the integrity and availability of the data.
- Data Curators – Involved with the design and integration between the Operating System and entities that contribute data. Responsible for the proper execution of the data curation process to include ongoing efforts to validate data, its usage, and continuous improvement. Establishment and maintenance of relationships with data providers.
- Data Architects – Responsible for the design and integration of all system back-end components.
- Data Stewards – Responsible for working with the Operating System to ensure that data is validated, categorized, and compliant with all agreements established at ingestion.

An individual may share one or more of these roles.

Chapter 2. References

Table 1: References lists documents and literature referenced during development of this DPP.

Table 1: References

Document Number	Title	Revision	Publication Date
N/A	Ben Green et al., "Open Data Privacy: A Risk-Benefit, Process-Oriented Approach to Sharing and Protecting Municipal Data," Berkman Klein Center https://cyber.harvard.edu/publications/2017/02/opendataprivacyplaybook	N/A	2/2017
N/A	Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, FIPS PUB 199. (2004). FIPS Pub 199 http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf	N/A	2/2004
N/A	Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, FIPS PUB 200. (2006). FIPS PUB 200 http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf	N/A	3/2006
N/A	Erica Kinkel, "Open Data Release ToolKit," DataSF https://datasf.org/resources/open-data-release-toolkit/	N/A	11/3/2016
N/A	Future of Privacy Forum, "City of Seattle Open Data Risk Assessment" https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf	N/A	1/2018
N/A	Khaled El Emam, "A De-Identification Protocol for Open Data," IAPP https://iapp.org/news/a/a-de-identification-protocol-for-open-data/	N/A	5/16/2016
800-60	National Institute of Standards and Technology (NIST), NIST Special Publication 800-60 Revision 1. (2008). NIST Special Publication 800-60 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf	N/A	8/2008
800-122	NIST Special Publication 800-122 https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf	N/A	4/2010

Document Number	Title	Revision	Publication Date
800-53	NIST Special Publication 800-53 Revision 4 (2013)[1] http://dx.doi.org/10.6028/NIST.SP.800-53r4	N/A	4/2013
800-188	NIST Special Publication 800-188, “De-identifying Government Datasets” https://csrc.nist.gov/csrc/media/publications/sp/800-188/archive/2016-08-25/documents/sp800_188_draft.pdf	N/A	12/15/2016
N/A	Official (ISC)^2 Guide to the CISSP CBK, Fourth Edition. (2015). ISC2 Press.	N/A	2015
N/A	The Privacy Act of 1974 (Title 5, U.S. Code, Sec. 552a) https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf	N/A	1974
N/A	The Common Rule (Title 45, Code of Federal Regulations (CFR), Part 46 (Protection of Data Subjects) https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html	N/A	1981
N/A	Ohio Revised Code § 1347: Personal information systems http://codes.ohio.gov/orc/1347	N/A	
N/A	Ohio Revised Code § 149.43: Availability of public records for inspection and copying http://codes.ohio.gov/orc/149.43	N/A	12/19/2016
N/A	“Protection of Human Subjects,” Title 49, CFR, Part 11 https://www.govregs.com/regulations/title49_chapterA_part11	N/A	1/15/2009
FHWA-JPO-17-461	THEA Connected Vehicle Pilot Data Privacy Plan, Phase 2, Task 2-C, FHWA-JPO-17-461 https://rosap.ntl.bts.gov/view/dot/32034	N/A	2/2017
FHWA-JPO-17-317	THEA Connected Vehicle Pilot Human Use Summary, Phase 1, Task 8, FHWA-JPO-17-317 https://rosap.ntl.bts.gov/view/dot/30926	N/A	7/2016
N/A	Smart Columbus System of Systems Concept of Operations, FHWA-JPO-18-635	N/A	1/12/2018
N/A	Smart Columbus Data Management Plan https://www.smartcolumbusos.com/share-your-data	N/A	6/07/2018, 9/28/2018, 12/31/2018, 1/29/2019, 8/19/2019, 8/07/2020

[1] *Smart Columbus is aware that NIST SP 800-53 Rev. 5 was recently released and that it is still in draft form. However, this particular document was not available at the time of development of the DPP. Smart Columbus may evaluate the changes to NIST SP 800-53 Rev. 5 at a future date and incorporate it into the DPP, as appropriate.*

Document Number	Title	Revision	Publication Date
N/A	Smart Columbus De-identification Policy https://www.smartcolumbusos.com/share-your-data	N/A	2019

Source: City of Columbus

Chapter 3. Principles and Legal Protections for Projects that Utilize Personally Identifiable Information

This Data Privacy Plan details the privacy and security controls for all aspects of the Smart Columbus data environment that collect, use, and/or share PII. To maintain focus on the importance of privacy and security, the City has aligned this plan with the following statement of principles that sets out Smart Columbus's strong commitment to privacy and data security. It then explains how Smart Columbus implements and achieves each of these principles and serves as a responsible data steward.

3.1. STATEMENT OF DATA STEWARDSHIP PRINCIPLES

To provide more efficient, equitable, and sustainable options, to improve the livelihood of Columbus residents, and to administer the program, Smart Columbus must collect, process, and share some participant personal information. Smart Columbus takes very seriously its obligation to respect individual privacy and to protect personal information. The following PII data privacy and security principles guide Smart Columbus in its collection and handling of personal information managed during the USDOT grant program and into the future:

- Smart Columbus does not collect, use, or share PII without the data subject's knowledge and informed consent.
- Smart Columbus collects and uses the minimum amount of PII necessary to satisfy the purposes of the demonstration.
- Smart Columbus uses and shares PII only for the specific purpose to which the data subject consented, or for other compatible purposes, and does so in ways that respect individual's reasonable expectations.
- Smart Columbus takes all reasonable measures to ensure the quality and validity of the information it uses.
- Smart Columbus retains PII only for so long as is necessary to accomplish the purposes for which it was collected or to accomplish other compatible purposes.
- Smart Columbus provides a mechanism for individuals to access, correct, and delete their PII.
- Smart Columbus takes reasonable data security measures to protect PII.
- Smart Columbus is as transparent as possible about its collection, use, maintenance, and disclosure of personal information, without revealing security measures.
- Smart Columbus institutes the processes necessary to hold itself accountable for compliance with these principles and with the project policies and procedure documents that implement them.
- Smart Columbus will notify affected individuals, USDOT, and the relevant IRB of the existence of, and its response to, data security breaches.

3.2. COMPLIANCE WITH APPLICABLE LAWS

Smart Columbus complies in all material respects with all applicable federal and state laws, rules, regulations, orders, and decrees including, but not limited to:

- The Privacy Act of 1974 (Title 5, USC, Sec. 552a)
- The Common Rule (Title 45, CFR, Part 46, Federal Policy for the Protection of Human Subjects)
- The Ohio Revised Code § 1347: Personal information systems
- The Ohio Revised Code § 149.43: Availability of public records for inspection and copying

3.3. PERSONALLY IDENTIFIABLE INFORMATION DEFINITIONS

In order to protect data as it enters the Smart Columbus program, the following definitions are used when reviewing each dataset for inclusion of PII.

- **Non-PII** is anything that is not PII. Encrypted data and data reasonably de-identified of PII and Sensitive Personally Identifiable Information (SPII) are Non-PII. Publicly-available PII is Non-PII for the purposes of this policy.
- **Publicly-Available PII** is PII that is lawfully available to the general public.
- **PII** is information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number (SSN), biometric records, location data, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, and mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified by examining the context of use and combination of data elements. Non-PII may become PII when additional information is made publicly available. This applies to any medium and any source that, when combined with other available information, could be used to identify an individual.
- **Sensitive PII (SPII)** is a subset of PII which, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data are compromised. The following PII is always (de facto) sensitive, with or without any associated personal information:
    - SSN
    - Passport number
    - Driver's license number
    - Vehicle Identification Number (VIN)
    - Biometrics, such as finger or iris print
    - Financial account number such as credit card, bank account number
    - Health information, including medical history, mental or physical condition, or medical treatment or diagnosis
    - Medicare status
    - Alien Registration Number

In addition to de facto Sensitive PII, some PII may be deemed sensitive based on context. Some PII becomes SPII when paired with another identifier, such as:

- Citizenship or immigration status
- Ethnic, religious, or sexual orientation or lifestyle information
- Last four digits of SSN
- Date of birth
- Criminal history
- Mother's birth name

Several Smart Columbus projects require that participants register which, by necessity, may include the collection of SPII. Protecting this data creates special considerations. SPII must be treated in accordance with federal, state and local laws, and the approved documents of the IRB.

Smart Columbus has established policies and procedures to ensure that PII and SPII can be protected in accordance with all applicable standards and documents. PII data is easily commingled with SPII in the context of the rapidly-moving exchanges taking place in the movement of data. Because of this, Smart Columbus treats all PII as SPII for the purpose of operational security controls. For access to data for use, PII and SPII are treated separately wherein role-based access controls are administered to provide appropriate differentiation.

This DPP discusses the policies, procedures, and security controls that are used in the protection of all participant PII and data subject information.

3.4. ADMINISTRATIVE AND LEGAL SAFEGUARDS

The Operating System team developed administrative and legal safeguards[2] to complement technical de-identification controls to protect data. Depending on the sensitivity and identifiability of the data, the Operating System employs mechanisms such as the following to set controls on Operating System datasets:

- **Contractual Provisions**: Data is made available to qualified users under legally binding contractual terms (such as commitments not to attempt to re-identify individuals or link datasets, to update the information periodically, or to use data in noncommercial and nondiscriminatory ways). Data may be backed up by audit requirements and penalties administered for noncompliance.
- **Data Access Controls**: This system allows data to be restricted to organizations or groups and authenticated users through different mechanisms.

3.5. SCOPE OF PLAN RELATED DEMONSTRATION DATA

While the DPP applies to all project-level data, there are projects where research is a main component, and data is collected and used outside of the immediate project team's review and the Operating System storage. This data may also be governed by the research entity's privacy policies, IRB oversight, and

[2] *Future of Privacy Forum, "City of Seattle Open Data Risk Assessment" (January 2018) p. 49-52 (https://www.seattle.gov/Documents/Departments/SeattleIT/DigitalEngagement/OpenData/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf)*

participant's consent. For example, in the PTA and MAPCD projects, meetings occurred with the researchers at OSU to review privacy policies.

Smart Columbus collects data both before and during the demonstration projects' life cycles. Some of this data, such as baseline data that existed prior to Smart Columbus, is already publicly available and may contain PII. For example, data that contains PII may be used to validate performance measures for a specific project. Data containing PII will not be ingested into the Operating System.

Chapter 4. Privacy Controls

The following Smart Columbus privacy controls are broadly guided by the USDOT-City of Columbus Cooperative Agreement, the Fair Information Practice Principles (FIPPs), and the NIST privacy-control catalog contained in Special Publication 800-53(r4) “Security and Privacy Controls for Federal Information Systems and Organizations” – Appendix J. The NIST Privacy Control Catalog applies to the majority of U.S. federal information systems. It provides agencies with a structured set of privacy controls, based on best practices, which help organizations comply with generally applicable, and organization-specific, privacy laws, and policies. The NIST privacy controls are consistent with and supplement those specified in the Cooperative Agreement. **Appendix B** summarizes how this DPP correlates to the NIST categories.

4.1. PRIVACY CONTROLS

In accordance with the Cooperative Agreement, Smart Columbus applies the following controls to all Smart Columbus data throughout the demonstration’s entire data life cycle and requires all sub-awardees and contractors to do the same.

4.1.1. Notice and Consent

Where possible, Smart Columbus provides timely, clear, and specific notice of its collection, use, and sharing of PII. Through various methods, Smart Columbus provides this notice, at the point of collection, to the individuals from whom the PII is being collected. Where notice at the point of collection is not possible, Smart Columbus provides clear and specific notice as soon as practicable.

For example, in the CVE project, prospective participants receive a clear and understandable presentation covering the privacy risks associated with joining the project. Only data that is necessary to get the participant into the informed consent process is collected prior to the execution of the informed consent, in accordance with procedures that have received advance approval from the demonstration’s IRB (see **Section 4.1.12**). Informed consent is predicated upon:

- Data to be collected
- The intended use and recipients of the data
- Clear notice of any privacy risks of participating, and of opportunities to opt out
- The general controls put in place to mitigate those risks
- All rights that participants hold over their own data

At the end of the presentation, each participant must sign a consent agreement to confirm their understanding of how the demonstration collects and uses PII and receive a description of the Smart Columbus privacy controls.

Smart Columbus demonstrations provide notice and informed consent pursuant to IRB- and/or USDOT-approved processes before collecting or using PII. Smart Columbus should provide such notice at the point of collection. For mobile applications such as the MMTPA, Smart Columbus obtains notice and informed consent through clear and concise opt-in privacy policies presented upon installation of the application. Informed consent isn’t applicable to several projects (e.g., SMH, CEAV). The IRB is informed of all expected participant uses and collected PII in the entire Smart Columbus program, so it can determine need for its oversight in each project.

4.1.2. Data Minimization

Smart Columbus projects collect and use only categories of personal information that are required to fulfill the grant objectives. A common best practice that reduces the negative consequences of a breach involving PII is for organizations to limit their PII collection to the least amount needed to accomplish legitimate purposes. Smart Columbus project managers identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of the project requirements.

4.1.3. Use and Sharing of Personally Identifiable Information

Smart Columbus uses and shares PII only as needed for the purpose provided via notice to the data subject, and to which the data subject consented, or for compatible purposes. In addition, Smart Columbus seeks to ensure that its use and sharing of PII is consistent with data subjects' reasonable expectations. Each demonstration project manager ensures that project PII is used only for specific purposes that are explicitly described in its privacy notices, or are compatible with the described purposes, and that are within the reasonable expectations of data subjects.

Demonstration data is shared only with authorized entities in service of legitimate demonstration purposes and subject to limitations on use and assurances that the privacy and security of the information will be protected in accordance with this DPP. Based on approval of the IRB and upon signing applicable data-sharing and use policies, Smart Columbus will provide certain demonstration data to the OSU project evaluators, subject to appropriate privacy and security safeguards, to ensure demonstration success.

Before Smart Columbus can use PII for purposes incompatible with those initially disclosed to individuals in privacy notices, it will need approval from the IRB, must provide the relevant data subjects with additional privacy notices, and receive their informed consent to the use of their data for the new purpose.

Smart Columbus does not use, sell, or distribute PII collected through the USDOT Smart Columbus program for any commercial marketing or advertising purposes. Smart Columbus uses PII only for Smart Columbus-authorized purposes.

In addition to the above-described purposes, Smart Columbus may use PII to the extent strictly required:

- To comply with applicable law or respond to valid legal process, including law enforcement or other government requests, but only to the extent strictly required to comply with such requests or processes;
- To protect the rights or interests of Smart Columbus, its partners, customers, individuals, or others, to prevent the loss of life or serious injury;
- To enforce Smart Columbus agreements, terms, or notices; or
- As otherwise described in its privacy notices.

4.1.4. Data Retention

Smart Columbus retains information only for so long as it needs to satisfy the purposes specified in its privacy notices, or for other compatible purposes, and in accordance with the applicable State of Ohio Public Records law and applicable contracts with third-party vendors. When PII is no longer necessary for the purposes specified in its privacy notices or for other compatible purposes, or at the conclusion of the project for which Smart Columbus collected the PII (whichever comes last), Smart Columbus will take reasonable steps to destroy, securely erase, or irreversibly de-identify all PII records in accordance with the Ohio-approved record retention schedule to prevent loss, theft, misuse, unauthorized access, or re-identification.

Among other reasons, Smart Columbus may also retain information to the extent strictly required:

- To comply with applicable laws or respond to valid legal process, including law enforcement or other government requests;
- To protect the rights or interests of Smart Columbus, its partners, customers, individuals, or others, to prevent the loss of life or serious injury;
- To enforce Smart Columbus agreements, terms, or notices; or
- As otherwise described in its privacy notices.

Smart Columbus might need to retain some categories of PII, such as registration and account information for continued routine operations and post-project administration. However, it only retains such PII in accordance with the privacy notices for each project. The privacy notices will specify the information categories that might be retained beyond the Smart Columbus demonstration lifetime.

As the volume of the data that the Operating System platform houses increases over time, data administrators will evaluate applying expiration policies to datasets or data within a dataset. This may include the moving of infrequently accessed data to other, less expensive storage or to make a recommendation to purge it in accordance to Ohio Public Records law requirements.

4.1.5. Access, Correction, and Deletion

Where feasible, Smart Columbus provides data subjects with a means to access, correct, and delete their PII that demonstration projects collect and use. Smart Columbus privacy notices and consent forms inform data subjects of these access, correction, and deletion opportunities, and of all other applicable rights under Ohio or federal law, as appropriate.

Through each project, Smart Columbus has established processes for receiving and responding to questions, concerns, and complaints from participants and data subjects in a reasonable, timely manner. Each process allows demonstration participants to:

- Request clarification on their data rights and Smart Columbus data uses and protections.
- Access and inspect their PII maintained in Smart Columbus information systems.
- Correct, update, and seek review of inaccurate or outdated PII that they have provided.
- Request information about any logged disclosure of their personal information held under Smart Columbus information systems as well as the date and recipient of that disclosure.
- Request to opt out or leave a demonstration project for which they have registered.
- Request deletion of existing PII and cease the collection of new PII after the participant has left a demonstration project. Where feasible and where data retention is not required, Smart Columbus may delete existing PII and cease to collect new PII if a participant leaves a demonstration project.

4.1.6. Transparency

As discussed in **1.4**, Smart Columbus is open about its information collection and use practices. It makes information available about its data collection and use practices to demonstration participants, residents, and interested parties through easily accessible mechanisms such as a public-facing website or information phone line staffed during normal business hours. In addition, as specified in **Section 4.1.7**, Smart Columbus is committed to providing individuals with timely, clear, and specific privacy notices.

4.1.7. Accountability

Smart Columbus has instituted the processes necessary to hold itself accountable for compliance with its data privacy principles and with the Data Privacy and Data Management controls that implement them.

Smart Columbus appointed resources to implement and monitor information security and information privacy protection in compliance with this DPP.

Smart Columbus developed an accountability process to ensure that PII is protected as designed, including documenting a Privacy Impact Assessment and conducting an annual, internal review of the DPP (or more frequently as required by law) and specifically, the controls, security measures and processes that protect PII.

Smart Columbus requires any vendors collecting PII on behalf of the program maintain a log of all disclosures to third parties of PII in its system. Smart Columbus will maintain this record for the lifetime of the demonstration, and it includes:

- The data, nature, purpose, and authority for each disclosure of records.
- The name and address of the person or agency to which the disclosure was made.

Smart Columbus will, upon request, make available to data subjects the accounting of disclosures to third parties.

4.1.8. De-Identification

According to NIST SP 800-122 (see **Appendix C**), generalizing, suppressing, introducing noise into, swapping, or replacing the data with the average value can introduce anonymity. Smart Columbus differentiates de-identification and anonymization. Anonymization implies re-identification is rendered impossible per NIST SP 800-188. Perfect anonymization is difficult, if not impossible. However, effective de-identification techniques reduce the chance for inadvertent exposure of a person's data. Smart Columbus chooses to use de-identification as the appropriate approach to protect personal information.

De-identification is applied to Smart Columbus data by de-identifying data with an appropriate technique relevant to the type of dataset and the authorized use. During data curation of datasets, the data is evaluated to see whether it contains PII information. If found to contain PII information, the dataset will be sent back to the provider for them to de-identify the data based on the Smart Columbus de-identification plan. The actual de-identification technologies and processes that Smart Columbus accepts are documented in the Smart Columbus De-identification Policy.

Data sourced from outside of the Operating System must follow the Smart Columbus De-identification Policy to be ingested. Once the data has been de-identified and analyzed for relevance and validity, it exists as "reasonably de-identified."

4.1.9. Data Curation

Data curation is a process wherein the Data Curator reviews each dataset, before being ingested into the Operating System, to ensure that a dataset does not include PII. The data curation ingestion process is further discussed in the DMP. Following are the privacy controls that are used by the Data Curator.

4.1.9.1. DATA INVENTORY

To develop appropriate and effective privacy controls, it is essential first to understand the data to which these controls apply. The first step in implementing such controls is, accordingly, to conduct a data inventory. In a dynamic program such as Smart Columbus, the data inventory will continue to evolve, since it is contingent on requirements and designs that are to follow in the systems engineering process. Smart Columbus created a data inventory to cover data that is or will be collected through the Smart Columbus program. The inventory contains the following information about each dataset: name, type, source, responsible party for maintenance, collection approach, frequency and period of collection, expected users, value of the data, whether the data contains PII, and where the data is located. The data inventory is attached as an Appendix to the Smart Columbus DMP which is available at https://www.smartcolumbusos.com/share-your-data.

A data inventory for the Operating System is available at www.smartcolumbusos.com/data.json. This is updated based on the standards set forward in the Smart Columbus DMP.

4.1.9.2. BENEFIT-RISK ANALYSIS

Reviewing datasets from a benefit-risk analysis is another way to protect the privacy of data. Following is the process that Smart Columbus uses to analyze data.

To add a dataset to the Operating System, a Smart Columbus Data Curator must complete and document the following process:

- **Step 1:** Evaluate the Information the Dataset contains.
- **Step 2:** Evaluate the Benefits.
- **Step 3:** Evaluate the Risks.
- **Step 4:** Weigh the Benefits against the Risks and Apply Appropriate Technical and Administrative Controls.

This process is informed by the work of: Future of Privacy Forum's Model Benefit-Risk Analysis; NIST SP-800-188 De-identifying Government Datasets; Khaled El Eman, A De-Identification Protocol for Open Data; the DataSF Open Data Release ToolKit; and the Berkman Klein Center's risk-benefit, process-oriented approach to sharing and protecting municipal data.

4.1.9.2.1 Step 1: Evaluate the Information the Dataset Contains

The Smart Columbus Data Curator reviews a dataset that has been submitted for inclusion in the Operating System, and classifies the information it contains by the following data categories:

- **Direct Identifiers:** Data points that identify a person without additional information or by linking to other readily available information such as names, SSNs, and employee ID numbers.
- **Indirect Identifiers:** Data points that do not directly identify a person, but that in combination can single out an individual. This could include information such as birth dates, ZIP codes, gender, race, or ethnicity.
- **Non-Identifiable Information**: Information that cannot reasonably identify an individual, even in combination and does not present privacy risks. For example, this might include city traffic patterns or atmospheric readings.
- **Sensitive Attributes**: Information that is sensitive in nature such as health conditions, financial information, and criminal justice records that should not be linkable to personal identities.
- **Special Data Categories**: Certain categories of information that are particularly difficult to de-identify such as geographic/location information, dates and times, unstructured or free form fields, biometric information, and photographs or videos and may require the application of de-identification tools.

4.1.9.2.2 Step 2: Evaluate the Benefits

Making datasets available in the Operating System can increase transparency, improve internal efficiency, and stimulate innovation, ideas, and services across an array of city challenges. For example, at the Smart Columbus Hackathon, civic innovators leveraged information from the Operating System to develop applications, tools, and services that will help:

- Manage city parking services.
- Share traffic information.
- Food insecure individuals/families find, share and/or access food assistance resources in central Ohio.
- Trip planning by routing individuals to appropriate transit options based on their mobility ability.
- Advise truck drivers of available spaces to stop for a break or to take their mandated rest.
- Inform oversized vehicle drivers of travel directions to avoid low clearance bridges.[3]

Various categories of information can also serve the purposes of government accountability, efficiency, analysis, and reporting.[4] The Smart Columbus Data Curator identifies which of the following groups may use a dataset and who stands to benefit from the data:

- Individuals
- Businesses, innovators, private entities
- Policymakers, researchers
- Civic data contributor/enthusiast
- Community groups
- Journalists[5]

Table 2: Value Analysis demonstrates assessment of the data value.

Table 2: Value Analysis

Likelihood of Occurrence	Low Impact of Foreseeable Benefits	Medium Impact of Foreseeable Benefits	High Impact of Foreseeable Benefits
Low	Low Benefit	Low Benefit	Medium Benefit
Medium	Low Benefit	Medium Benefit	High Benefit
High	Medium Benefit	High Benefit	High Benefit

Source: City of Columbus

[3] *Smart City Hackathon (May 18-20) (https://scos.splashthat.com/')*

[4] *DataSF "Open Data Release Toolkit: Privacy Edition" p. 22 (https://datasf.org/resources/open-data-release-toolkit/)*

[5] *Ben Green, Gabe Cunningham, Ariel Ekblaw, Paul Kominers, Andrew Lizer and Susan Crawford, "Open Data Privacy Playbook," Berkman Klein (Feb. 27, 2017), p. 15 (https://cyber.harvard.edu/publications/2017/02/opendataprivacyplaybook)*

4.1.9.2.3 Step 3: Evaluate the Risks

Each dataset contemplated for addition to the Operating System must be evaluated for any risks that data may create. Following are the risk categories that are assessed against each dataset:

- **Re-Identification:** Even when a dataset has been de-identified of names and other potentially identifying traits and rendered "de-identified," there is a chance that someone might be able to deduce that some of the data relates to a specific individual. This is an extremely difficult, technical task to attempt automatically. These risks may rise over time as additional information is added to the portal, or there are advances in re-identification technologies. The responsibility of the Operating System is to inform those managing data of the potential opportunity for re-identification when datasets are added or modified in the system. Re-identification could harm individuals or organizations through:
  - Exposure to the risk of identity theft, discrimination, or abuse.
  - Revealing location information that could lend itself to burglary, property crime, or assault.
  - Exposing a person to financial harms or loss of economic opportunity.
  - Causing embarrassment or psychological harm.
- **Data Quality and Equity**: In some circumstances, the consequences of inaccurate, incomplete, or biased data can lead to group-level risks such as:
  - Creating or reinforcing biases towards or against a particular group.
  - Disproportionately including or excluding information from a particular group in the dataset in a way that causes poor policymaking or inequitable distribution of services.
- **Public Trust Impacts:** Even if properly de-identified or aggregated, making certain types of datasets publicly available may engender public opposition. The Smart Columbus Data Curator considers:
  - Does a dataset contain sensitive types of information that could lead to public opposition?
  - Public expectations as to how the particular dataset will be used or shared.
  - Is it likely that the information in the dataset will lead to a chilling effect on individual, commercial, or community activities, particularly activities protected by the First Amendment?
  - Could third parties use the data set improperly?

Table 3: Risk Analysis demonstrates assessment of the risk of ingestion.

Table 3: Risk Analysis

Likelihood of Occurrence	Low Impact of Foreseeable Risks	Medium Impact of Foreseeable Risks	High Impact of Foreseeable Risks
Low	Low Risk	Low Risk	Medium Risk
Medium	Low Risk	Medium Risk	High Risk
High	Medium Risk	High Risk	High Risk

Source: City of Columbus

4.1.9.2.4 Step 4: Weigh the Benefits against the Risks, Apply Appropriate Technical and Administrative Controls

Table 4: Benefits and Risks of Dataset Inclusion demonstrates weighing the benefits against the risk of including a dataset in the Operating System.

Table 4: Benefits and Risks of Dataset Inclusion

Benefit	Low Risk	Medium Risk	High Risk
High Benefit	Add data to operating System subject to appropriate controls.	Add data to Operating System subject to appropriate controls.	Possibly add data and consider heightened controls. Possibly consider public awareness campaign.
Medium Benefit	Add data to Operating System subject to appropriate controls.	Possibly add data and consider heightened controls. Possibly consider public awareness campaign.	Do not release data.
Low Benefit	Possibly add data and consider heightened controls. Possibly consider public awareness campaign.	Do not release data.	Do not release data.

Source: City of Columbus

4.1.9.3. DATA QUALITY

Smart Columbus ensures information originated from the demonstration environment that will be used by demonstration projects is valid, fresh, and complete for the purposes specified in its privacy notices. For complete details about how Smart Columbus ensures valid, fresh, and complete information, see the Smart Columbus DMP.

4.1.10. Privacy Testing

Good policy maintains that every process is tested for success. For data that is ingested into the Operating System, the following tests have been and will continue to be conducted to reduce the likelihood of PII being introduced to the Operating System and that re-identification of the ingested data is improbable.

4.1.10.1. RE-IDENTIFICATION RISK TEST

Smart Columbus will apply a re-identification risk test every 6 months to determine whether any data presents a risk of re-identification. The test would simulate the activities of a person who starts without any prior knowledge but wishes to identify an individual from personal data that was de-identified on the Operating System. This test is meant to assess whether the person would be successful.[6]

[6] *UK, Information Commissioners Office "Anonymisation: Managing Data Protection Risk Code of Practice" (https://ico.org.uk/media/1061/anonymisation-code.pdf)*

This test could include the following examples:

- A web search to discover whether a combination of date of birth and postcode data can be used to reveal a particular individual's identity;
- Searching the archives of a national or local newspaper to see whether it is possible to associate a victim's name with crime map data;
- A social network search to see if it is possible to link de-identified data to a user's profile; or
- Using the electoral register and local library resources to try to link de-identified data to someone's identity.[7]

4.1.10.2. DE-IDENTIFICATION VALIDATION

Smart Columbus periodically reviews ingested data for unintended inclusion of PII. Smart Columbus selects a sampling of datasets and reviews each by field level to determine if the dataset included any PII.

4.1.11. Compartmentalization

Smart Columbus may also use a concept called compartmentalization. Compartmentalization is the partner to role-based access discussed earlier. Information is divided into compartments to keep any one entity from having the entire picture. This keeps the data compartmentalized such that only the role with access to both project data and PII can make the correlation.

4.1.12. Institutional Review Board

Title 49, CFR, Part 11 codifies the USDOT-adopted Common Rule, which provides guidance on defining when a project falls under the rule, and associated requirements, for approvals, oversight, and IRB involvement. Because Smart Columbus is federally funded and involves the use of participants, approval of human use by an IRB is required.

Smart Columbus data security and participant PII are under the oversight of the IRB. IRB approval will be determined within each of the constituent projects as well as at the program-level for any activities involving human subjects. For example, performance measurement activities such as general program-wide surveys of the Smart Columbus demonstration will not be distributed until such approval is received.

Documents for submission to the IRB have been developed for each project, with oversight by an IRB compliance consultant, and will include the research protocol documents, participant recruitment plans, informed consent documents, training plans and materials, and ongoing amendments as needed. A Human Use Approval Summary report has been delivered to USDOT covering the entirety of the ongoing IRB process.

IRB approval is subject to ongoing and periodic review as progress advances past concept development and into the details of recruitment, screening, registration, PII data storage, training, and message sharing with participants. Treatment of Smart Columbus participant data, especially of vulnerable populations, depends on project provisions made through the project-specific, IRB-approved informed consent and research protocol documents.

The IRB has general oversight of treatment of participants with respect to equity, safety, beneficence, and informed consent. Participants must be treated fairly and equitably, fully informed of the study goals,

[7] *El Emam, A De-identification Protocol for Open Data" IAPP (May 2016) (https://iapp.org/news/a/a-de-identification-protocol-for-open-data/)*

aware of what their participation involves, the study risks, their legal rights, who to contact with questions, and their ability to withdraw and the procedure to withdraw from the demonstration at any time. Informed consent includes discussion of the uses of participant data and ensure that participant data is understandable to project participants. Interpreters and/or translations are provided as determined by the IRB for fairness and vulnerable populations as well as providing reasonable means to participate to the general population.

Smart Columbus submits periodic updates to the IRB to revise the project-specific research protocol documents and informed consent documents as the Smart Columbus demonstration progresses.

4.1.13. Control Boards

Smart Columbus has empaneled IRB professionals from Advarra and The Ohio State University to be the IRB of record depending on the project. The IRBs fulfill the requirements of an IRB under the Federal Policy for the Protection of Human Subjects (“Common Rule”), U.S. Department of Health and Human Services’ Title 45, CFR, Part 46, and the USDOT’s Guidance Summary for Connected Vehicle Deployments, Human Use Approval (FHWA-JPO-16-346). The USDOT’s Guidance Summary for Connected Vehicle Deployments, Human Use Approval (FHWA-JPO-16-346) is available on the USDOT CV Pilots’ website.[8]

The role of the IRB is to administer the approval of all informed consent forms and privacy agreements (e.g., website privacy notice, application, kiosk click-through terms of service, or posting in an autonomous vehicle) relating to participation in specific projects and collection and use of personal data through the Smart Columbus demonstration. Further, the IRB:

- Reviews and approves privacy notices and data uses for demonstration projects involving projects that use data subjects.
- Receives notice of security or privacy incidents as well as resolution and status.
- Authorizes any disclosures of Smart Columbus data to third parties.

Smart Columbus will empanel a five-member Privacy and Security Board, made up of three privacy professionals and two security professionals in central Ohio. This Board will advise Smart Columbus on privacy and security issues. The City will appoint volunteer board members for two-year terms or until Smart Columbus ceases operations. The Privacy and Security Board will:

- Advise Smart Columbus on new developments and emerging best practices in information privacy and security.
- Recommend, where relevant, and advise upon any modifications to the DPP.
- Receive notice of security or privacy incidents as well as resolution and status.
- Annually review any audits or assessments conducted through the year.

4.1.14. Project Evaluator’s Access to Data

Smart Columbus has a Performance Measurement Plan (PfMP) that details how the Operating System and each project will measure their performance.

The Operating System is used to house, publish, and distribute Smart Columbus program performance measure data and categorizes the data as public or restricted. Authorized users from OSU who are

[8] https://www.its.dot.gov/pilots/phase1_technical.htm

conducting project evaluations require access to data collected specifically pursuant to the PfMP. The data that is categorized as public or restricted is available to OSU project evaluators through the Operating System user interface and through an API to query the data. Project evaluators collect data containing PII directly due to the prohibition of PII in the OS.

4.1.15. Contractors and Other Third Parties

Smart Columbus has established privacy roles, responsibilities, and access requirements for any sub-recipients, contractors, and service providers that may interact with demonstration PII. Smart Columbus will attach this DPP to all sub-recipient, contractor, or service provider contracts where the sub-recipient, contractor, or service provider collects, maintains, possesses, accesses, uses, stores, or destroys personal information collected through the demonstration for the Smart Columbus program. These entities will comply in all material respects with the security and privacy requirements of this DPP and the USDOT Cooperative Agreement.

4.1.16. Privacy Impact Assessments and Risk Governance

Privacy Impact Assessments (PIAs) are structured processes for identifying and mitigating privacy risks, including risks to confidentiality, within an information system. The Chief Security Officer established a risk governance process to facilitate vendors and project participants through the PIA. The Smart Columbus team conducts a project-appropriate PIA for each Smart Columbus demonstration project and for partners collecting PII on behalf of the project. After the PIA, Smart Columbus assigns a risk level through an assessment summary which is shared with the project team. The project team and vendors are responsible for validating the accuracy of the assessment. Program management is responsible for risk treatment and can address or accept the risks for each demonstration project. The Smart Columbus team will conduct additional PIAs if a vendor or project team begins collecting PII, or if the risk level increases later due to PII collection. **Appendix A** includes a PIA example.

Chapter 5. Security Controls

Data security is fundamental to public confidence in Smart Columbus project demonstrations and the overall success of the program's objectives. While no information system can guarantee that a breach will never happen, the Smart Columbus team views data security as a foundational principle. It is dedicated to ensuring that all Smart Columbus data, including PII, will be stored only on IT infrastructure that employs security controls commensurate with the risk to the individual that would result from unauthorized access, disclosure, or use of the information.

Information Security is based on maintaining the AIC Triad: availability, integrity, and confidentiality of information. The AIC Triad is sometimes referred to as the CIA Triad. The Smart Columbus approach to system threat assessment, analysis of application flows, and device classifications is based on the process defined by the Federal Information Processing Standards (FIPS) Publications 199 and 200.

5.1. SECURITY CONTROLS OVERVIEW

Three types and three means comprise security controls. The three types of controls are:

1. **Preventive:** Put in place to inhibit harmful events.
2. **Detective:** Put in place to discover harmful events.
3. **Corrective:** Put in place to restore systems after harmful events.

These security controls follow a progression from blind optimism (believing that prevention will eliminate all negative events) to the sky is falling (we cannot stop them, better prepare to pick up the pieces). The best security plans utilize a balance of the available controls to accomplish the best solution based on multiple factors including:

- Risk tolerance of data owner.
- Value of data at risk.
- Damage expected from loss or exposure.
- Likelihood of loss or exposure.
- Cost of various safeguard options compared to the level of assurance they bring and the above factors.

Smart Columbus identifies and manages security controls following the steps recommended by NIST in its FIPS SP 800-53 Document, and the Smart Columbus systems requirements are constructed around these steps:

- Categorize the demonstration information systems containing PII as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability based on FIPS Publication 199 impact assessment (partially completed by USDOT – pre-award, preliminary reassessment based on current state of design at point of DPP creation, and another reassessment to follow final design).
- Select the applicable security control baseline based on the results of the security categorization and apply tailoring guidance (including the potential use of overlays).

- Implement the security controls and document the design, development, and implementation details for the controls.
  - Assess the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system and examining all hardware elements within the network that serve as potential points of entry or vulnerable to entry.
- Authorize information system operation based on a determination of risk to organizational operations and assets, individuals, other organizations resulting from the operation and use of the information system and the decision that this risk is acceptable.
- Monitor the security controls in the information system and environment of operation on an ongoing basis to determine control effectiveness, changes to the system/environment, and compliance to legislation, policies, regulations, and standards.

5.2. MEANS OF CONTROL

The means for implementing controls are:

- **Administrative:** Includes policies and procedures, security awareness training, background checks, and levels of supervision.
- **Logical or Technical**: Targets the restriction of access and includes encryption, smart cards, access control lists, and biometrics, etc.
- **Physical**: Incorporates security guards, alarm systems, locks, etc.

5.3. SECURITY CONTROLS

The development and application of security controls and standards for Smart Columbus demonstration data are based on the recommendations of NIST 800-122 “Guide to Protecting the Confidentiality of PII” and NIST 800-53 “Security and Privacy Controls for Federal Information Systems and Organizations” (see **Appendix C**).

Consistent with the Cooperative Agreement to meet the minimum-security baselines for demonstration PII as required by USDOT, Smart Columbus:

- Protects all PII, electronic and hardcopy, in its custody from unauthorized disclosure, modification, or destruction so that the confidentiality, integrity, and availability of the information are preserved.
- Stores PII only on IT infrastructure employing security controls commensurate with the risk to the individual that would result from unauthorized access, disclosure, or use of the information.
- Encrypts all PII in transit or at rest.
- Encrypts all PII transmitted or downloaded to mobile computers/devices.
- Ensures that all individuals having access to PII have received training in the policies and procedures that protect PII.

5.3.1.1. ENCRYPTION

All data collected through Smart Columbus projects that contain PII are encrypted while in transit and at rest. Because reasonably de-identified data has already had all PII/SPII removed by the application of a technical filter, it is the only form of data permitted to be stored or transmitted in clear text or as appropriate. 256-bit Advanced Encryption Standard (AES) encryption is used for all other data types. Where reasonably possible, encryption in transit and at rest is used for all types of data.

5.3.1.2. PHYSICAL CONTROL

The technical means of data and privacy protection are only as secure as the physical means preventing access to stored or live data. For example, requiring an extremely sophisticated password schema is of insignificant effect if user passwords are widely known to be written and stored in an unlocked desk drawer. The Smart Columbus Chief Security Officer ensures that staff who have access to PII are professionally trained on using physical protection methods to protect against physical exposure of original data containing PII that hasn't been de-identified. Example of physical devices and data include computer storage devices and hard-copy paper records. Further physical controls include alarm systems, cabinet locks, and security background checks.

5.3.1.3. ACCESS CONTROL – REMOTE ELECTRONIC ACCESS TO DEVICES AND SYSTEMS

All access to project data via electronic means is protected by an access-control system including identification, authentication, role-based authorization, access, and event logs to allow internal review.

5.3.1.4. AUTHORIZATION – ID-BASED

Authorization occurs after authentication. Whereas the authentication establishes the identity of person requesting access, authorization based on ID determines the level of access to be granted. All access to any level of project data begins at this ID-based authorization. A Privileged ID Management (PIDM) system may be implemented in the later phases of the Operating System development.

Authorization details have been developed as Smart Columbus progresses and include:

- Multifactor authentication to access PII. This protects the data from phishing attacks, which is a prominent method for gaining unauthorized access to sensitive data. This is the kind of protection used to access personal bank accounts and electronic medical records, and it is appropriate for use to access stored PII.
- The creation, storage, and protection of keys is a vital component in keeping data safe. Commonly accepted algorithms, key length, key exchange, or other areas that could lead to the defeat encryption systems.
- Managers or delegated staff to periodically review the access privileges of each of their associates to ensure they are authorized for the role.
- A process/technology to ensure access is removed quickly if someone is terminated and altered if someone takes a new role.
- An enforced password policy consistent with industry-accepted best practices. The policy should include, at a minimum:
  - Periodic change or higher complexity requirements such as passphrases.
  - A set number of failed login attempts results in account being locked.
  - Set time period for login attempts to include minimum and maximum time intervals.
  - Enforced password complexity.

5.3.1.5. AUTHORIZATION – ROLE-BASED

In addition to the ID-based authorization above, personnel access to PII should be further restricted based on specific job roles within the project. For example, the staff involved in the registration of participant data shall not be involved in the collection or analysis of other project data, and the staff involved in analyzing project data shall not have access to participant data. This precludes staff with project data access from being able to extrapolate PII from project data via comparison with the registrant data. The goal is to mitigate situations where de-identified data could potentially be re-identified.

Throughout the project there may be situations where an examination of both project data and registrant data is required. Designated project staff with adequate training, as approved by the IRB, are responsible for the protection of human subjects throughout the project. These staff comprise a limited number of individuals for each Smart Columbus project.

5.3.1.6. PENETRATION TESTING

Ethical hackers under the authority of project management have conducted, and will conduct as necessary, penetration testing on the Operating System. These ethical hackers operate outside of the sphere and influence of the system architecture design and implementation for the sole purpose of identifying vulnerabilities and exploits within the system. During and after system design and deployment, the penetration testers will attempt to break down any of the three tenets of the AIC Triad. By providing this type of targeted attack by safe sources, the team can better prevent or mitigate malicious or inadvertent outside attacks. Smart Columbus promptly made reasonable efforts to rectify vulnerabilities and exploitations discovered through penetration testing.

5.3.1.7. SECURE SOFTWARE DEVELOPMENT LIFECYCLE

Software built to process or store PII implements security controls within the Software Development Life Cycle (SDLC) using a combination of either manual or automated controls as appropriate. For example, code reviews can be employed either manually or using automation tools such as Static and Dynamic Code Analysis. As appropriate, software is built in a way to mitigate the Open Web Application Security Project (OWASP) Top 10 Most Critical Web Application Security Risks. Programming software and libraries are monitored for security vulnerabilities and updated as security fixes are published.

5.3.1.8. SECURITY OPERATIONS

Both passive and active system monitoring controls are implemented for the system architecture in environments containing PII or environments accessible on the internet. These monitoring applications examine system activity for anomalies and other signs of improper operation or possible system exploits. These systems may have a corrective component that automatically implements safeguards to inhibit further exploit or may simply alert project staff of the event so that manual action can be affected. These systems may include network monitoring, data-sniffers, key loggers, Simple Network Management Protocol traps (send alerts to management system regarding suspicious traffic), Access Control Lists (hardware monitoring rule configuration), vulnerability scanning, and others. These controls are provided by information and network security systems, such as firewalls, web application firewalls, file integrity monitors, intrusion detection, and prevention systems. Higher risk alerts identified via these controls send notifications to a chat system or mobile telephone that is monitored and responded to by qualified personnel.

5.3.1.9. DATA LOSS PREVENTION

Data Loss Prevention (DLP) technologies are implemented to reduce the likelihood of loss of PII during processing. These controls can include:

- Restrict internal resources from emailing a file with more than “X” PII records embedded. “X” should represent an exceedingly small number of records that could be downloaded.
- Restrict internal resources from copying a file with “X” PII records to a USB drive or send out via email.
- If associates are permitted to copy files to a USB drive, allow use of only a specific encrypted USB drive.
- Lock down any computers provided for PII to only allow work-related access. If possible, shutdown the USB ports, eliminate the ability to copy files to the local drive, do not allow web-based email, etc.

5.3.1.10. PATCHING, ANTIVIRUS, AND MALWARE CHECKING

Antivirus and malware-checking software is utilized for each system component as appropriate. Antivirus and malware-checking applications are primarily detective in that they recognize and report code patterns associated with potential exploits. These are most effective for open networks in which access control is weak. While the Smart Columbus communication system and network are actively secured, antivirus and malware checking software is still deployed on workstations, servers, and other systems commonly affected by malware such as Microsoft Windows Operating Systems where inadvertent introduction of hostile code could occur. Demonstration personnel apply patches to servers and desktop computers in alignment with vendor updates.

5.3.1.11. TRAINING

Any Smart Columbus personnel or individuals who may have access to PII such as software developers, system testers, and project managers will be required to complete training covering the security policies, procedures and requirements of this DPP. The Chief Security Officer manages this. The Chief Privacy Officer ensures that the training includes data privacy policies and procedures. The training communicates the importance of protecting PII and builds knowledge and skills that enable Smart Columbus personnel to protect the security and confidentiality of PII in accordance with the DPP. Training should target the employees’ levels without unnecessarily complicating the tasks to recall or exposing privileged knowledge of the system.

The training includes:

- Instruction in specific privacy and security control mechanisms.
- Role-based privacy and security training.
- Individual certification of acceptance of privacy responsibilities.
- Periodic refresher courses and re-certification.
- ORC 1347 Personal Information Systems.
- ORC 149.43 Availability of Public Records for Inspection and Copying.

Any Smart Columbus personnel that interact with project-specific research data involving human subjects are required to complete the Collaborative Institutional Training Initiative (CITI) Human Subjects training course prior to being approved as a data reviewer through the IRB process.

5.3.1.12. ASSESSMENTS AND EVENT REVIEW

5.3.1.12.1 Independent Security and Privacy Advisory Board

Smart Columbus institutes the processes necessary to hold itself accountable for compliance with its data privacy principles and with the Data Privacy and Data Management plans that implement them.

The Security and Privacy Advisory Board serves as an additional means to provide independent perspective to Smart Columbus on the success of the Data Privacy Plan.

Due to the sheer volume of data that will be amassed and the potential for human error, independent board review of documentation artifacts, assessments, and other audit trails can help ensure policy adherence for availability, integrity, and confidentiality.

Documentation artifacts reviewed by the Security and Privacy Board can include the IRB's required research protocol documents, informed consent documents, Privacy Impact Assessments, security policies, and access logs. Section **4.1.12.** discusses the role of the IRB.

5.3.1.12.2 Security Operations Event Review

System elements generate system events, access, and administrative logs for staff. Smart Columbus monitors the events to ensure security controls are effectively protecting PII as designed. As defined in Section **5.3.1.9**, Smart Columbus analyzes information system events for indications of compromise, inappropriate, or unusual activity affecting PII and take any necessary restorative and preventative actions.

5.3.1.12.3 Incident Response

Smart Columbus will follow the below Privacy and Security Incident Response Plan that includes training for all staff in the proper procedures for reporting a breach or suspected breach of PII data. Smart Columbus will:

- Notify the Chief Security and Privacy Officers and Smart Columbus leadership of any suspected or actual privacy breach or system compromise.
- Assess scope of impact of the incident by Chief Security and Privacy Officers.
- Create an incident response team that will investigate and document the incident, preserve evidence, eliminate any ongoing risks, and determine what, if any, violations have occurred.
- Promptly report any suspected loss of control of PII, system breach or failure by Smart Columbus, its subgrantees, or contractors that does not result in the unauthorized disclosure of PII. This could include suspected unauthorized collection, use, maintenance, dissemination, or deletion of PII.
    - Reportable to USDOT Agreement Officer
- Promptly report any unauthorized disclosure of PII by Smart Columbus, its subgrantees, or contractors. This could include actual unauthorized collection, use, maintenance, dissemination, or deletion of PII.
    - Reportable to USDOT Agreement Officer, IRB, law enforcement (as appropriate).
    - For PHI, reporting to Health and Human Services (HHS) Office of Human Research Protections (OHRP) is expected within one month when adverse events that are Unanticipated Problems (UP), such as data breaches, occur. The IRB may undertake this reporting.

  - Any unauthorized disclosure of privacy data will also require notification of participants and any State of Ohio authority as determined in the legal compliance review by City of Columbus.
- Retain all reports in this section in the project records according to the requirements of the applicable Smart Columbus record retention schedule.

Appendix A. Privacy Impact Assessment

The criteria shown in **Table 5**: Privacy Impact Assessment Outline of Required Contents is used for evaluating project privacy impact.

Table 5: Privacy Impact Assessment Outline of Required Contents

Section 1.0: Characterization of Information		**Response**
1.1	What information is collected, used, disseminated, or maintained in the system?	
1.2	What are the sources of the information in the system?	
1.3	Why is the information being collected, used, disseminated, or maintained? Is there a specific legal mandate or business purpose that requires the use of this information?	
1.4	How is the information collected?	
1.5	What specific legal authorities, arrangements, and/or agreements defined the collection of information?	
1.6	Conclusion: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.	
Section 2.0: Uses of the Information		
2.1	Describe all the uses of information.	
2.2	How will the information be checked for accuracy and/or validity?	
2.3	What types of tools are used to analyze data and what type of data may be produced?	
2.4	If the system uses commercial or publicly-available data please explain why and how it is used.	
2.5	Conclusion: Describe any types of controls that may be in place to ensure that information is handled in accordance with the described uses in 2.1.	
Section 3.0: Retention		
3.1	What information will be retained?	
3.2	How long will information need to be retained?	
3.3	Has the retention met the NARA records schedule?	
3.4	Is the information deleted in a secure manner?	
3.5	Conclusion: Please discuss the privacy risks associated with the length of time data is retained and how those risks are mitigated.	

Section 1.0: Characterization of Information		Response
Section 4.0: Internal Sharing and Disclosure		
4.1	With which internal City or demonstration entities is the information shared, what information is shared, and for what purpose?	
4.2	How is the information transmitted or disclosed?	
4.3	Conclusion: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.	
Section 5.0: External Sharing and Disclosure		
5.1	With which external organization(s) is the information shared, what information is shared, and for what purpose?	
5.2	Is the sharing of personally identifiable information outside the demonstration compatible with the original collection? If so, is it addressed in a data-sharing agreement? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of the demonstration.	
5.3	How is the information shared outside the agency and what security measures safeguard its transmission?	
5.4	How does the agency verify that an external organization has adequate security controls in place to safeguard information?	
5.5	Conclusion: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.	
Section 6.0: Notice		
6.1	Was notice provided to the individual prior to collection of information?	
6.2	Do individuals have the opportunity and/or right to decline to provide information?	
6.3	Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?	
6.4	Conclusion: Describe how notice is provided to individuals, and how the privacy risks associated with individuals being unaware of the collection are mitigated.	
Section 7.0: Access, Redress, and Correction		
7.1	What are the procedures that allow individuals to gain access to their information?	
7.2	What are the procedures for correcting inaccurate or erroneous information?	
7.3	How are individuals notified of the procedures for correcting their information?	

Section 1.0: Characterization of Information		Response
7.4	If no formal redress is provided, what alternatives are available to the individual?	
7.5	Conclusion: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.	
Section 8.0: Security Implementation		
8.1	What procedures are in place to determine which users may access the system and are they documented?	
8.2	Will contractors have access to the system?	
8.3	Describe what privacy training is provided to users either generally or specifically relevant to the program or system?	
8.4	What auditing measures and technical safeguards are in place to prevent misuse of data?	
8.5	Does the project employ technologies which may raise privacy concerns? If so, please discuss their implementation.	
8.6	Conclusion: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?	

Source: City of Columbus

Appendix B. National Institute of Standards and Technology Special Publication 800-53 Control Categories

NIST SP 800-53 specifies a list of control categories to be included in a DPP. **Table 6**: National Institute of Standards and Technology Control Categories Correlation illustrates how the DPP correlates to the NIST categories.

Table 6: National Institute of Standards and Technology Control Categories Correlation

NIST Category	DPP Section(s)	NIST Objective	Verification Method/Outcome
AP Authority and Purpose			
AP-1 Authority to Collect	**4.1.7 Accountability** **4.1.12 Institutional** Review B	Determine and document the legal authority that permits the collection, use, maintenance, and sharing of PII either generally or in support of a specific program or information system need.	- Does the DPP cite its authority to collect PII data?
AP-2 Purpose Specification	**4.1.1 Notice and Consent**	Describe purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices.	- Does the DPP provide purpose(s) for PII usage? - Do informed consent documents disclose purpose(s) for which data will be used?
AR Accountability, Audit, and Risk Management			
AR-1 Governance and Privacy Program	**Executive Summary**	Identify individual to monitor and enforce privacy policies and to monitor federal privacy laws and policies for changes that affect the SC program's privacy policies.	- Has an individual been identified to monitor and enforce privacy policies for the project?
AR-2 Privacy Impact and Risk Assessment	**Chapter 4. Privacy Controls**	Verify the creation and implementation of a privacy risk-management process and related PIAs.	- Has SC created and implemented a privacy risk-management process and related PIAs? - Assess the most likely threat scenarios: - Malicious outsider attempting to steal PII

NIST Category	DPP Section(s)	NIST Objective	Verification Method/Outcome
			• Malicious outsider attempting to commit fraud or steal funds. • Negligent insider being compromised. • Malicious insider attempting to steal PII or commit fraud.
AR-3 Privacy Requirements for Contractors and Service Providers	**Executive Summary**	Verify the establishment of privacy roles, responsibilities, and access requirements for contractors and service providers; and includes privacy requirements in contracts and other acquisition-related documents.	• Do contractor and service providers' contracts and other acquisition-related documents contain privacy requirements? • Do systems include and enforce permission-based roles for any contractor or service provider users? • Are all contractors and service providers given documentation regarding their responsibilities and access restrictions with regards to PII?
AR-4 Privacy Monitoring and Auditing	**4.1.10 Privacy Testing**	To monitor and audit privacy controls and internal privacy policy to ensure effective implementation.	• Internal Audits o Is there a method for periodic internal audits in alignment with Performance Measurement and Evaluation Support Plan (PMESP) requirements? o Is there budget and staff assigned for internal audits? o Is there a process to resolve audit findings? o How many internal audits are scheduled? o How many internal audits have been performed? • External Audits o Is there a method for periodic external audits in alignment with PMESP requirements? o Is there budget and resources identified for external audits? o How many external audits are scheduled? o How many external audits have been performed?
AR-5 Privacy Awareness and Training	**5.3.1.11 Training**	Verify the establishment and implementation of privacy protection	• Does the training provided to study staff include content regarding privacy protection

NIST Category	DPP Section(s)	NIST Objective	Verification Method/Outcome
		training, along with documented staff acceptance of privacy protection responsibilities.	policies and practices as well as documented staff acceptance of appropriate responsibilities?
AR-6 Privacy Reporting	**5.3.1.12 Assessments and Event Review**	The development, distribution, and updating of reports that demonstrate compliance with The Ohio State University or Advarra IRB.	• Are reports of privacy plan changes and/or system breaches shared in all cases and within stated timeframes? • Are reports retained in accordance with NARA requirements?
AR-7 Privacy-Enhanced System Design and Development	**Chapter 4. Privacy Controls**	Verify that information systems support privacy by automating privacy controls.	• Anonymity ○ Is live data, accessed in the field on OBUs, RSUs, or sniffers – protected according to the stated security standards? ○ Is stored CV raw data protected against unauthorized dissemination and intrusion according to the stated methods? ○ Is ID-based/role-based authorization required to access the following? ○ Live or stored connected vehicle (CV) data (original and de-identified) ○ PII data in any state • Filtering/Scrubbing ○ Has “de-identified” CV data been cleared of data identified in the project as ‘sensitive’? • Need to Know ○ For all systems collecting, transmitting, or storing CV, PII, or participant data – is all access restricted by an assigned system-enforced role? • Compartmentalization ○ According to Smart Columbus standards, are data types in all systems that collect, transmit, or store data properly separated from each other? (i.e.: raw data is not

NIST Category	DPP Section(s)	NIST Objective	Verification Method/Outcome
			available to users of de-identified data etc.)
AR-8 Accounting of Disclosures	**5.3.1.12 Assessments and Event Review**	Track information disclosed from each system of record including date, nature, and purpose of each disclosure as well as the name and address of the person or agency receiving the information. Also verify that this audit trail is retained for the life of the record or five years after the disclosure is made. Also verify that the audit trail of disclosures is made available to the person named in the record upon request.	• Are internal disclosures within the SC team documented and available for IRB audit? • Are unauthorized disclosures tracked and reported?
DI Data Quality and Integrity			
DI-1 Data Quality	**4.1.9.3 Data Quality**	Verify that the program confirms the accuracy, relevance, timeliness, and completeness of PII upon collection or creation, collect PII directly from the individual as much as possible, checks for and corrects as needed – any inaccurate or outdated PII used by SC programs or systems.	• Has the SC program provided the ability for individuals to enter their own PII directly? • Does the Smart Columbus program provide a method by which individuals can update their PII?
DI-2 Data Integrity and Data Integrity Board	**Chapter 4. Privacy Controls**	Document processes to ensure the integrity of PII through existing security controls.	• Does the system used to collect and store PII have controls applied to protect the integrity of the data? • Does it protect against unauthorized access? • Does it protect against unauthorized PII modification? • Does it a process for to validate the accuracy of PII?
DM Data Minimization and Retention			
DM-1 Minimization of	**3.1 Statement of Data**	Identify the minimum PII that is necessary to	• Does the program only gather the PII identified in the DPP?

NIST Category	DPP Section(s)	NIST Objective	Verification Method/Outcome
Personally Identifiable Information	**Stewardship Principles** **4.1.2 Data Minimization**	accomplish the project goals, limit the collection and retention of PII to those minimum elements, and conduct an initial evaluation of PII holdings and follow a regular schedule for reviewing those holdings to ensure that only PII identified as minimum required data is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.	• Has the program conducted an initial review of PII holdings to ensure that only PII identified as minimum-required data is collected and retained? • Does the program periodically review its PII data categories to ensure that they remain required to accomplish its legally-authorized purpose?
DM-2 Data Retention and Disposal	**Chapter 4. Privacy Controls**	Verify that the SC program retains PII to fulfill stated purpose for the PII, that the project disposes of the PII in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access and uses identified methods to ensure secure deletion when destroying PII.	• Is PII data used to exclusively fulfill its stated purpose in the project? • Once the PII's usage is complete, is PII disposed of in a NARA-approved method?
DM-3 Minimization of PII Used in Testing, Training, and Research	**3.1 Statement of Data Stewardship Principles** **4.1.2 Data Minimization**	Verify the development of policies and procedures that minimize the use of PII for testing, training and research. Verify that controls have been implemented to protect PII used for testing, training, and research.	• Do policies and procedures exist that minimize the use of PII? • Have the controls enumerated in the DPP been implemented?
IP Individual Participation and Redress			
IP-1 Consent	**Chapter 4. Privacy Controls**	Verify that the project has provided a means for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection.	• Does the method of signing up new participants include an explicit authorization from those individuals regarding PII collection? • Does the method of signing up new participants include a summary of consequences

NIST Category	DPP Section(s)	NIST Objective	Verification Method/Outcome
		Verify that the project has provided a means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use dissemination and retention of PII.	regarding either the approval or the rejection of PII collection?
IP-2 Individual Access	**4.1.5 Access, Correction, and Deletion**	Verify that the project provides individuals the ability to have access to their PII maintained in its system(s) of records. Verify that the project publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of record as appropriate.	
IP-3 Redress	**4.1.5 Access, Correction, and Deletion**	Verify that the project provides a process for individuals to have inaccurate PII corrected.	• Does the project provide a method for participants to correct their PII?
IP-4 Complaint Management	**4.1.6 Transparency**	Verify that the project has implemented a process for receiving and responding to complaints, concerns, or questions from individuals about the project's privacy practices.	• Does the project provide a method for participants to lodge complaints, concerns, or questions regarding privacy practices? • How many complaints have been received during the span of the study? • How many questions have been received during the span of the project? • Of the complaints received, what percentage have been resolved? • Of the questions that have been received, what percentage have been answered?
SE Security			
SE-1 Inventory of Personally Identifiable Information	**4.1.9.1 Data Inventory**	Verify that the project has established and updated an inventory containing a listing of all	• Has the project program established an inventory of all systems and programs that

NIST Category	DPP Section(s)	NIST Objective	Verification Method/Outcome
		programs and information systems that collect, use, maintain, or share PII, and that this inventory is shared with the CIO or Information Security Official for the project.	collect, use, maintain, or share PII? • Does the program maintain that inventory on a periodic basis? • Has that inventory been shared with the individual charged with managing security for the program?
SE-2 Privacy Incident Response	**Chapter 4. Privacy Controls**	Verify that the project has developed and implemented a Privacy Incident Response Plan and does provide an organized and effective response to privacy incidents in accordance with the plan.	• Does the SC program have a Privacy Incident Response Plan? • How many incidents have been logged since the inception of the study program? • On average, how many days elapsed between the detection of the incident and the final response?
TR Transparency			
TR-1 Privacy Notice	**Chapter 4. Privacy Controls**	Verify that the project provides effective notice to the public and to individuals regarding its activities that impact privacy, including its collection use, sharing, safeguarding, maintenance, and disposal of PII its authority for collecting PII, and the ability to access and have PII corrected. Verify that the project describes the PII collected and its purpose, how the project uses the PII, whether the project shares PII with external entities, how individuals may obtain access to PII, and how the PII will be protected. Verify that the project revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact	• Does the program effectively notify participants of its activities that impact privacy? • Does the program share with participants the types of PII that is collected, the purpose for collection, if the PII will be shared with third parties, how the data will be secured, and how it will be eventually disposed of? • Have the program’s processes or practices regarding PII changed, and have its public notices been updated accordingly?

NIST Category	DPP Section(s)	NIST Objective	Verification Method/Outcome
		privacy – in a timely manner.	
TR-2 System of Records Notices and Privacy Act Statements	**N/A**		
TR-3 Dissemination of Privacy Program Information	**4.1.6 Transparency**	Verify that the project ensures that the public has access to information about its privacy activities and is able to communicate with its senior agency official for privacy.	• Does the project or its sponsor, USDOT, ensure that the public has adequate access to information with regards to PII used in the project? • Does the public have access to the individual assigned to manage privacy for the project?
UL Use Limitation			
UL-1 Internal Use	**Chapter 5. Security Controls**	Verify that the project uses PII internally only for the authorized purpose identified in public notices and the Privacy Act.	• Does the project use PII internally according to its stated authorized purpose?
UL-2 Information Sharing with Third Parties	**Chapter 5. Security Controls**	Verify that Smart Columbus shares PII only for the authorized purposes. Verify that the project monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII, and that the project evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.	• Does the project consistently filter/scrub data prior to sharing with third parties? • Audit SCMS Certificates/CRL • Do logs exist? Do they show a pattern of attempted intrusion? • Encryption ▪ Is live data encrypted? ▪ Is stored raw CV data encrypted? ▪ Is data in transit encrypted? ▪ Is all PII data encrypted? ▪ Is electronic participant data encrypted? • Access Control – Physical ▪ Is physical access to the following devices protected according to the project's stated standards? ▪ Devices collecting or transmitting CV data of any kind. ▪ Devices storing raw or de-identified CV data.

NIST Category	DPP Section(s)	NIST Objective	Verification Method/Outcome
			▪ Devices collecting, transmitting, or storing PII or SPII ▪ Are all hard-copy documents containing participant data under physical protection according to the project's stated standards? • Access Control – Remote ▪ Is remote access to the following devices protected according to the project's stated standards? ▪ Devices collecting or transmitting CV data of any kind. ▪ Devices storing raw or scrubbed CV data. ▪ Devices collecting, transmitting or storing PII or SPII. • Penetration Testing ▪ What is the frequency of penetration testing? ▪ What is the number of systems tested? ▪ What is the number of systems with high-risk findings? ▪ What is the number of findings per system? ▪ What is the number of closed finding per system? • System Monitoring ▪ Are systems that collect, transmit, or store CV data monitored according to the SC program's stated practice? ▪ How many systems are being monitored? ▪ What is the average system availability to date? ▪ How many intrusions have system monitors logged to date?

NIST Category	DPP Section(s)	NIST Objective	Verification Method/Outcome
			▪ How many blocked intrusions have system monitors logged to date? • Antivirus ▪ Do all systems that transmit or store CV or participant data have up-to-date antivirus protection? ▪ How many malware incidents have been logged by antivirus software per system?

Source: City of Columbus

Appendix C. National Institute of Standards and Technology Special Publication 800-122 Checklist Summary

Table 7: National Institute of Standards and Technology Checklist

Checklist Question	DPP Consideration
Has your organization ever performed work for a federal agency that involved handling PII?	Yes. **The City handles federal tax information governed by IRS Publication 1075. IRS Contact: Jackie Nielson, Fed State Coordinator, Ohio District Department of the Treasury, (614) 280-8739.**
Does your organization have any policies/procedures to protect the security and confidentiality of PII?	Yes. **The City has Executive Orders, policies and procedures to protect the security and confidentiality of PII. City Executive Orders and Policies are posted at [https://www.columbus.gov/hr/Executive-Orders-and-Policies/.](https://www.columbus.gov/hr/Executive-Orders-and-Policies/)**
Does your organization have any policies/procedures to control and limit access to PII?	Yes. **The City has Executive Orders and Policies to control and limit access to PII. City Executive Order and Policies are posted at [https://www.columbus.gov/hr/Executive-Orders-and-Policies/.](https://www.columbus.gov/hr/Executive-Orders-and-Policies/)**
Does your organization store PII on network drives and/or in application databases with proper access controls (i.e., User IDs/passwords)?	Yes. **The City assigns unique identifiers and requires complex passwords.**
Does your organization limit access to PII only to those individuals with a valid need to know?	Yes. **The City limits access to PII only to those individuals with a valid need to know.**
Does your organization prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants, which are generally higher risk than nonportable devices (e.g., desktop computers at the organization's facilities)?	Yes. **Executive Order 2007-03 prohibits such actions.**
Does the information system used by your organization to store PII contain automated or easy-to-use process to ensure that only authorized users access PII – and only to the extent that each user has been authorized to do so?	Yes. **The City uses Active Directory to assign unique identifiers, require complex passwords and control access to private or sensitive information.**
Does your organization monitor events that may affect the confidentiality of PII, such as unauthorized access to PII?	Yes. **The City monitors events and configures alerts for events that may affect the confidentiality of PII.**

Checklist Question	DPP Consideration
Does your organization audit its information systems on a regular or periodic basis?	Yes. **The City performs security assessments by various methods including access, rule, and configuration reviews. The City is also subject to external audits including an IRS Safeguards Review.**
Does your organization analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions?	Yes. **The City has a Security Incident Response Plan written to provide a well-defined, organized approach for handling any potential threat to systems and data.**
Does your organization restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm)?	Yes. **The City maintains strict control over the internal or external distribution of any kind of media. Digital containing sensitive information is physically secured from unauthorized access, labeled, inventoried, and is tracked via logs. Non-digital media containing sensitive information is only kept when necessary for business purpose and physically secured from unauthorized access.**
Does your organization restrict access to portable and mobile devices capable of storing PII?	Yes. **Executive Order 2007-03 prohibits copying sensitive information to such devices.**
Does your organization require that information system media and output (such as printed documents) containing PII be labeled to indication appropriate distribution and handling?	Yes. **PO 22 requires that media must be classified so that the sensitivity of the data can be determined.**
Does your organization securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures?	Yes. **Physical and logical access to media containing PII is strictly controlled. Encryption is used on digital media.**
Does your organization sanitize digital and nondigital media containing PII before disposing of or reusing the media?	Yes. **Paper media is destroyed using crosscut shredders. Digital media is sanitized prior to reuse or destroyed as part of disposal.**

Source: City of Columbus

Appendix D. Acronyms and Definitions

Table 8: Acronym List contains program level acronyms used throughout this document.

Table 8: Acronym List

Acronym/Abbreviation	Definition
AIC	Availability, Integrity, and Confidentiality
AES	Advanced Encryption Standard
API	Application Programming Interface
BRT	Bus Rapid Transit
CEAV	Connected Electric Autonomous Vehicles
CFR	Code of Federal Regulations
CIA	Confidentiality, Integrity, and Availability
CITI	Collaborative Institutional Training Initiative
CMAX	Brand for COTA Cleveland Avenue Bus Rapid Transit
COTA	Central Ohio Transit Authority
CRL	Certificate Revocation List
CV	Connected Vehicle
CVE	Connected Vehicle Environment
DLP	Data Loss Prevention
DMP	Data Management Plan
DPP	Data Privacy Plan
EPM	Event Parking Management
FHWA	Federal Highway Administration
FIPPs	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
HHS	Health and Human Services
ID	Identification
IRB	Institutional Review Board
IT	Information Technology
ITS	Intelligent Transportation Systems
JPO	Joint Program Office
MAPCD	Mobility Assistance for People with Cognitive Disabilities

Acronym/Abbreviation	Definition
MMTPA	Multimodal Trip Planning Application
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OBU	(DSRC) Onboard Unit
OHRP	Office of Human Research Protections
ORC	Ohio Revised Code
OSU	The Ohio State University
OWASP	Open Web Application Security Project
PIA	Privacy Impact Assessment
PIDM	Privileged Identification Management
PII	Personally Identifiable Information
PMESP	Performance Measurement and Evaluation Support Plan
PTA	Prenatal Trip Assistance
RSU	(DSRC) Roadside Unit
SC	Smart Columbus
SCC	Smart City Challenge
SCMS	Security and Credentials Management System
SDLC	Software Development Life Cycle
SMH	Smart Mobility Hubs
SoS	System of Systems
SPII	Sensitive Personally Identifiable Information
SSN	Social Security Number
UP	Unanticipated Problems
USB	Universal Serial Bus
USC	United States Code
USDOT	United States Department of Transportation
USDOT-JPO	United States Department of Transportation – Joint Program Office
VIN	Vehicle Identification Number
ZIP	Zone Improvement Plan

Source: City of Columbus

Appendix E. Glossary

Table 9: Glossary contains project specific terms used throughout this document.

Table 9: Glossary

Term	Definition
Access Control Terms	• **Identification:** The means by which users claim their identities to a system. Identity is a required precursor to authentication and authorization. • **Authentication:** The testing or reconciliation of evidence of a user's identity. IT established and verifies that a user is who they say they are. • **Authorization:** The right and privileges granted to a person or process. • **Accountability:** The processes and procedures by which a system obtains its ability to determine the actions and behavior of a single individual or process within the system and to identify that individual person or process. Audit trails and logs are examples of tools supporting accountability.
Aggregated Data	Information is summarized across the population and released as a report of those statistics. Does not contain PII.[9]
Agile	A method of project management that is characterized by the division of tasks into short phases of work and frequent reassessment and adaptation of plans.
App	Software application.
Data Subject	Refers to the subject of PII used by Smart Columbus.
Drivers	The drivers (residents and visitors) in Columbus who will be interacting with the Smart Columbus projects.

Source: City of Columbus

[9] *Green et al., p. 27*

SM
RT
COLUMBUS

THE CITY OF
COLUMBUS
ANDREW J. GINTHER, MAYOR