NYC OTI
Office of Technology & Innovation

Agency Privacy Officer Toolkit

Version	Description of Change	Approver	Date
3.0	Added privacy impact assessment template. Revised Identifying Information Rider and Privacy Protection Rider and added supplemental materials to support execution of new terms. Incorporated instructions for requesting deviations from the Identifying Information Rider and for requesting best interests of the City determinations. Added and expanded guidance on contextual integrity, privacy-enhancing techniques and technologies, and assessing the use of online analytics. Added guidance and sample materials for obtaining consent related to data and for drafting program-specific privacy policies. Revised Model Investigation Plan and sample notification letter. Added template for receiving complaints from the public	Michael Fitzpatrick Chief Privacy Officer, City of New York	January 28, 2025
2.0	Added comprehensive model compliance plan checklists, model guidance and reference documents section, and model investigation plan. Incorporated former contracts toolkit material. Migrated and updated Identifying Information Rider, Privacy Protection Rider, and related contract materials from Citywide Privacy Protection Policies and Protocols	Michael Fitzpatrick Chief Privacy Officer, City of New York	February 6, 2023
1.0	First Version	Laura Negrón Chief Privacy Officer, City of New York	June 14, 2019

Page Intentionally Blank

Message from the Chief Privacy Officer

Dear colleagues,

I am pleased to share the latest Agency Privacy Officer Toolkit and 2025 update to the Citywide Privacy Protection Policies and Protocols. These documents serve as the foundation for privacy practices across city agencies.

Within the toolkit, you will find comprehensive resources including privacy by design guidance, ensuring new tools and programs have built in safeguards to protect privacy throughout our operational and administrative processes from the beginning. Also included is a template privacy policy for use when creating new programs or services, guidance creating a citywide standard for consent regarding data use, and for the first time, a Privacy Impact Assessment template to analyze the impact of handling identifying information. We have also included updated templates for contracts and agreements that set standards for privacy protection in data-sharing activities both within city agencies and with external partners.

I strongly encourage you to review these policies and leverage the toolkit to ensure your agency remains in compliance with privacy laws and regulations, as well as integrates best practices in privacy protection. Thank you for your ongoing work in safeguarding the privacy of New Yorkers. By working together, I am confident we will continue to set the standard for privacy protection.

Sincerely,

Michael Fitzpatrick
Chief Privacy Officer
City of New York

Agency Privacy Officer Toolkit

Overview

This toolkit is designed to help agency privacy officers effectively implement the Identifying Information Law and Citywide Privacy Protection Policies and Protocols.

It contains compliance checklists, templates for data sharing agreements, nondisclosure agreements, and scopes of work, as well as guidance for handling and investigating security incidents. In addition, the toolkit provides tools to help privacy officers build relationships with executive staff and employees, such as sample agendas and template letters.

Please visit the Office of Information Privacy's intranet page for supplemental material, annotated and editable versions of the documents contained in the toolkit, and contact information for all of the City's agency privacy officers.

Table of Contents

Key Features of the Citywide Privacy Protection Policies and Protocols	
Section	**Summary Description**
Privacy Principles (Sec. 2.0)	A set of principles that should be incorporated into all aspects of agency decision-making where privacy interests may be implicated. Includes: (1) Transparency (2) Public Trust (3) Accountability (4) Data Minimization (5) Use Limitation (6) Responsible Governance and Stewardship (7) Data Quality, Integrity, and Accuracy (8) Security Safeguards (9) Equity
"Sensitive" Identifying Information (Sec. 3.2.11)	Refers to certain types of identifying information the agency privacy officer or Chief Privacy Officer has determined pose a higher risk of harm if improperly disclosed.
Relationship with Other Laws and Policies (Sec. 1.5, 1.6)	Clarification of the relationship between the Chief Privacy Officer Policies and Protocols with other relevant laws (e.g., Freedom of Information Law, the City's Open Data Law, and the City's data breach notification law) and City policies (e.g., the Citywide Cybersecurity Program Policies and Standards).
Clarification of Terms Not Defined in the Identifying Information Law (Sec. 3.2)	Provides interpretation of key terms not defined in the Identifying Information Law: • Anonymization • Collection, disclosure, use, and access • Complaint • Exigent circumstances • Sensitive identifying information • Requests and proposals
Agency Liaison Network (Sec. 4.2.3)	Requires agency privacy officers to establish working relationships with key agency stakeholders and describes these stakeholders' agency roles.
Approval of Collections and Disclosures (Sec. 4.3)	Recommends agency privacy officers to approve only collections or disclosures respecting the contextual integrity of identifying information and defines key terms relating to contextual integrity.

Key Features of the Citywide Privacy Protection Policies and Protocols	
Section	**Summary Description**
Privacy by Design (Sec. 4.3.1)	Recommends that agencies use privacy by design processes in the development of systems, applications, or services that processes identifying information.
Individual Consent (Sec. 4.3.2)	Describes the guidelines for obtaining and approving consent for the collection, use, or disclosure of identifying information.
Guidance for Making "Routine" Designations by Agency Function (Sec. 5.1.2)	Advises that for routine collections and disclosures, agencies should have protocols to ensure the appropriate level of legal review before making the collection or disclosure.
Case-by-Case Collections and Disclosures (Sec. 5.2)	Describes agency privacy officer role in reviewing and approving case-by-case collections or disclosures; sets forth considerations for agencies in determining whether a collection or disclosure should be designated as routine or non-routine.
Reporting Collections and Disclosures Made Under Exigent Circumstances (Sec. 5.4.1)	Agency staff must report collections and disclosures made under exigent circumstances to agency privacy officers as soon as practicable, and agency privacy officers must report such collections and disclosures to the Chief Privacy Officer within 24 hours of discovering the collection or disclosure, except where exempted under Admin. Code § 23-1202(d)(1).
Privacy-Enhancing Techniques and Technologies (Sec. 5.6)	Recommends using privacy-enhancing techniques and technologies to minimize the collection, use, and disclosure of identifying information.
Program-Specific Privacy Policies (Sec. 5.8)	Describes the process for creating, updating, and maintaining program-specific privacy policies using collaboration between agency privacy officers and various stakeholders to ensure accuracy, legal compliance, and alignment with data practices.
Modifications to the Identifying Information Rider (Sec. 6.1.3)	Describes the process for requesting approval to modify the Identifying Information Rider.
Data Sharing Agreements (Sec. 6.2)	Describes when a written data sharing agreement is needed and the key elements of such agreements.

Key Features of the Citywide Privacy Protection Policies and Protocols	
Section	**Summary Description**
Elements of Data Sharing Agreements (Sec. 6.2.2)	Data sharing agreements involving identifying information should include several elements, including a requirement to cooperate with City investigations into unauthorized disclosures.
Review by Law Dept. of Agreements (Sec. 6.2.3)	Unless otherwise determined by the Law Department, requires agencies to consult with the Law Department for agreements involving the disclosure of identifying information to external parties to determine whether additional provisions, such as indemnification, insurance, and intellectual property, may be appropriate.
Complaint and Investigation Mechanism (Sec. 8.0)	Requires agencies to establish a mechanism for accepting and investigating reports of suspected or known violations of the Identifying Information Law.
Receiving Complaints (Sec. 8.2)	Requires agencies to adopt protocols for receiving and investigating complaints, which must include cooperating with the Chief Information Security Officer and other key agencies, including the Chief Privacy Officer, the Law Department, and Office of Cyber Command (**Cyber Command**).
Notification of Received Complaints (Sec. 8.2.1)	Agency privacy officers must notify the Chief Privacy Officer within 24 hours of any known improper use, disclosure of, or access to identifying information.

Model Compliance Plan

Instructions

This section is a model compliance plan that agency privacy officers can use or modify to comply with Citywide Privacy Protection Policies and Protocols (**CPO Policies**) Section 4.2.2, which requires agency privacy officers to develop a plan for following the Identifying Information Law.

The plan is composed of a set of checklists. Each checklist lists tasks that agency privacy officers complete to comply with the Chief Privacy Officer Policies and Protocols. The *Once Per Agency Checklist* and *Once Per Agency Privacy Officer Checklist* are designed to assist new agencies and new agency privacy officers, respectively, while the remaining checklists are intended for use by all new and existing agencies and agency privacy officers.

Many of the tasks have associated templates and reference documents that agency privacy officers can adapt for their use. For updated and annotated documents, as well as supplemental materials, please visit the Office of Information Privacy's intranet page.

Once Per Agency Checklist					
🕑 *Frequency*: When a new agency is created.					
	Task	**Description**	**Completed**	**Date**	**Reference**
(1)	Designate an agency privacy officer.	• Each agency head must designate an agency privacy officer, with consultation from the Chief Privacy Officer. • When a new agency privacy officer is designated, the agency must notify the Chief Privacy Officer by email at oip@oti.nyc.gov, and provide the agency privacy officer's contact information.	☐		N/A
(2)	Implement an agency privacy protection policy.	• Agencies must comply with the CPO Policies. They may adopt supplemental policies that address their needs. • Agency privacy officers should become familiar with the Citywide Cybersecurity Program Policies and Standards.	☐		Model Compliance Plan CPO Policies 1.5.3
(3)	Determine and preapprove routine collections and disclosures of identifying information.	• Agency privacy officers should pre-approve collections and disclosures of identifying information relating to normal agency business operations as routine designations. • Agency privacy officers should document routine designations on Form 2.	☐		Form 2

Once Per Agency Checklist					
🕑 *Frequency*: When a new agency is created.					
(4)	Implement process for receiving reports of violations of the IIL.	• Agency privacy officers must implement a process to receive and review reports of violations of the Identifying Information Law.	☐		Model Investigation Plan CPO Policies 8.2

Once Per Agency Privacy Officer Checklist					
🕑 *Frequency*: Once each time a new agency privacy officer is designated.					
	Task	**Description**	**Completed**	**Date**	**Reference**
(1)	Receive agency privacy officer training.	• The Office of Information Privacy provides one-on-one training for each new agency privacy officer. Self-schedule training with the Office of Information Privacy or contact oip@oti.nyc.gov.	☐		N/A
(2)	Meet with the Chief Privacy Officer.	• The Chief Privacy Officer meets with each new agency privacy officer. Self-schedule a meeting or contact oip@oti.nyc.gov.	☐		N/A
(3)	Review existing routine and case-by-case approvals of collections and disclosures.	• New agency privacy officers should review and update their agencies' existing approved collections and disclosures of identifying information.	☐		Biennial Agency Report Form 2 Form 5
(4)	Meet with agency head.	• Agency privacy officers are key figures in their agencies' decision-making processes around identifying information. Each agency head should know who the agency privacy officer is and should understand the agency privacy officer's role within the agency.	☐		Agency Head Template Agenda

Once Per Agency Privacy Officer Checklist					
🕑 *Frequency*: Once each time a new agency privacy officer is designated.					
	Task	**Description**	**Completed**	**Date**	**Reference**
(5)	Send introduction to agency staff.	• Agency privacy officers play an important role in identifying and handling information within their agency. They rely on accurate and current information to make decisions, issue policies, and report on privacy practices. They should also make themselves known to staff and be transparent about their agency's privacy needs.	☐		APO Template Introductory Email
(6)	Identify and meet with agency chief information security officer.	• Intra-agency networks, especially between privacy and security, can help agency privacy officers understand their agency's challenges and improve coordination on privacy and other areas.	☐		CISO Template Agenda
(7)	Identify and meet with agency business unit heads.	• Agencies cannot collect or disclose identifying information without approval from their agency privacy officers. Agency privacy officers should have strong relationships with business unit heads so that they are aware of business decisions that affect their agencies' collections and disclosures of identifying information.	☐		Sample Template Meeting Agenda

Once Per Month Checklist					
🕑 *Frequency*: Once per month.					
	Task	**Description**	**Completed**	**Date**	**Reference**
(1)	Meet with agency chief information security officer.	• Strong intra-agency networks, especially at the intersection of privacy and security, help agency privacy officers understand the issues facing their agencies and improve agencies' coordination on privacy, security, risk management, incident response, and other areas.	☐		CISO Template Agenda
(2)	Meet with agency business unit heads.	• Agencies cannot collect or disclose identifying information without approval from their agency privacy officers. Agency privacy officers should have strong relationships with business unit heads so that they are aware of business decisions that affect their agencies' collections and disclosures of identifying information.	☐		Sample Template Meeting Agenda

Once Per Quarter Checklist					
🕑 *Frequency*: Once per quarter.					
	Task	**Description**	**Completed**	**Date**	**Reference**
(1)	Report violations of the Identifying Information Law and collections and disclosures of identifying information made under exigent circumstances.	• Email oip@oti.nyc.gov to report whether the agency violated the Identifying Information Law. • Email oip@oti.nyc.gov to report whether the agency collected or disclosed identifying information under exigent circumstances. • Email oip@oti.nyc.gov to report that the agency neither violated the Identifying Information Law nor collected or disclosed identifying information under exigent circumstances.	Mar. 31 ☐ June 30 ☐ Sept. 30 ☐ Dec. 31 ☐		Identifying Information Law Notification Form
(2)	Brief agency head on existing and potential privacy issues.	• Agency privacy officers are important in identifying information and making decisions within their agency. Each agency head should know their agency's privacy officer and understand the agency privacy officer's role. • Use meetings to learn about and update the agency head on privacy issues and potential impacts of agency strategic directions.	☐		Agency Head Template Agenda

Once Per Year Checklist					
🕑 *Frequency*: Once per year.					
	Task	**Description**	**Completed**	**Date**	**Reference**
(1)	Send privacy guidance to staff.	• Agency privacy officers must remind employees about following the Identifying Information Law and how to contact the agency privacy officer.	☐		Model Guidance to Agency Staff
(2)	Train staff on privacy protection.	• Agency privacy officers must ensure that employees understand how to identify and handle identifying information, how to report suspected violations of the Identifying Information Law, and other basic privacy practices. • Agencies may use the citywide training developed by the Office of Information Privacy and may require supplemental privacy training. • Agency privacy officers should be familiar with Cyber Command's cybersecurity awareness training, which is intended to help employees become aware of potential threats that could result in an incident or compromise the availability or integrity of identifying information to which an employee may have access.	☐		DCAS Citywide Training Module Cybersecurity Awareness Training

Once Per Year Checklist					
🕑 *Frequency*: Once per year.					
(3)	Review existing routine and case-by-case approvals of collections and disclosures.	• Agency privacy officers should review and update their agencies' existing approved collections and disclosures of identifying information.	☐		Biennial Agency Report Worksheet 1 Worksheet 2 Form 2 Form 5
(4)	Conduct an incident response tabletop exercise.	• Agency privacy officers must practice using their agencies' incident response plans and process for reviewing complaints of violations of the Identifying Information Law. • It is important for agency privacy officers and chief information security officers to work together on tabletop exercises because it allows them to identify potential vulnerabilities and develop strategies for responding to various types of threats and incidents, which helps to improve the overall security posture of the agency and protect sensitive information. • Consider conducting a single joint tabletop exercise with the agency's chief information security officer.	☐		Model Investigation Plan Citywide Incident Response Policy Agency Incident Response Readiness Program
(5)	Review the agency's privacy impact assessments	• Agency privacy officers should review their agency's privacy impact assessments annually to ensure they are accurate.	☐		Privacy Impact Assessment

Once Every Two Years Checklist					
🕑 *Frequency*: Once every two years.					
	Task	**Description**	**Completed**	**Date**	**Reference**
(1)	Update agency-wide inventory of identifying information practices.	• Agency privacy officers should review and update their agencies' existing approved collections and disclosures of identifying information.	☐		Worksheet 1 Worksheet 2 Form 2 Biennial Agency Report Form 5
(2)	Prepare and submit the agency report.	• Agencies must submit reports on their privacy practices by July 31 every two years to the Chief Privacy Officer, Citywide Privacy Protection Committee, the Mayor, and the Speaker of the City Council.	☐		Biennial Agency Report

Ongoing Tasks and Responsibilities			
🕑 *Frequency*: Ongoing.			
	Task	**Description**	**Reference**
(1)	Review agency requests for routine and case-by-case approvals for collections or disclosures of identifying information.	• Agency privacy officers must approve or deny requests for collections or disclosures of identifying information. For example, when a new initiative is proposed or new category of identifying information is added to a process, agency privacy officers must review the request, consider the privacy policies and principles, and make and record their determinations. • Agency privacy officers should be familiar with the Citywide Cybersecurity Program Policies and Standards.	Form 2 Form 5 Citywide Cybersecurity Program Policies and Standards
(2)	Review Chief Privacy Officer-designated non-routine disclosures of identifying information.	• Agencies should document review and approval status on Form 5.	Form 5
(3)	Receive and review complaints related to of the Identifying Information Law.	• Agency privacy officers must handle complaints related to the Identifying Information Law where identifying information was collected or disclosed in violation of the Identifying Information Law. Agency privacy officers should ensure there is a mechanism to receive such complaints and address them, whether they are identified by other colleagues or by the public.	Identifying Information Law Notification Form Model Investigation Plan

Ongoing Tasks and Responsibilities			
🕑 *Frequency*: Ongoing.			
(4)	Notify the Chief Privacy Officer of collections and disclosures made under exigent circumstances or disclosures in violation of the Identifying Information Law within 24 hours of discovery.	• Agency privacy officers must notify the Chief Privacy Officer within 24 hours when they become aware of a collection or disclosure under exigent circumstances or a disclosure in violation of the Identifying Information Law. This should be done using the IIL Notification Form. • Agency privacy officers should also coordinate with agency chief information security officers to coordinate notification to Cyber Command about potential cybersecurity incidents.	Identifying Information Law Notification Form
(5)	Collaborate with agency counsel, chief information security officer, and business heads to comply with the Identifying Information Law, implement privacy best practices in contracts and memoranda of understanding, and responding to inquiries.	• Agency privacy officers should build relationships with internal stakeholders to protect privacy in their agencies' practices and agreements.	Contracts and Agreements
(6)	Create and update privacy impact assessments.	• Agency privacy officers should work with agency staff to conduct a privacy impact assessment before the agency implements a new project that changes how the agency collects, uses, or discloses identifying information. Revise it as needed if there are changes to how identifying information is processed by the project.	Privacy Impact Assessment

Model Guidance and Reference Documents

Instructions

This section contains documents that agency privacy officers may find helpful and can use for the tasks outlined in the Model Compliance Plan. Agency privacy officers are free to change or supplement these documents as they see fit. For updated and annotated documents, as well as supplemental materials, please visit the Office of Information Privacy's intranet page.

Guidance on Implementing Privacy by Design

Instructions

This section provides a structured approach for implementing a privacy by design framework when designing a system, project, or service that involves identifying information. Agency privacy officers are encouraged to use this approach for coordinating with legal, technical, and business stakeholders to design appropriate privacy controls to be deployed for projects that involve identifying information. This guidance complements the City's existing privacy and cybersecurity directives, including Citywide Cybersecurity Program Policies and Standards and the Citywide Privacy Protection Policies and Protocols, and should be used alongside other resources. Agencies are encouraged to tailor this privacy by design approach to align with their specific agency workflows, operational needs, and risk profiles.

Agencies may be required to obtain additional business, legal, and technical approvals that are not contained in this document before designing or releasing systems, projects, or services.

Privacy by Design Chart		
🕑*Frequency*: Once each time a new project involving identifying information is initiated.		
	Action	**Description**

(1)	Engage Stakeholders from the Outset.	• Identify and involve key stakeholders early in the planning phases of any project that processes identifying information.
		  ○ Key stakeholders will likely include agency privacy officers, legal counsel, technical staff, cybersecurity professionals, and project managers.
		  ○ Initial consultation with agency privacy officers helps create an early project framework that complies with privacy regulations, including the Identifying Information Law.

(2)	Begin a Privacy Impact Assessment.	• A privacy impact assessment is recommended when designing projects that collect or disclose identifying information. ○ Privacy impact assessments help define and evaluate projects' privacy risks against the privacy laws, regulations, and contracts that govern them. • It is good practice to conduct a privacy impact assessment early to guide design decisions and update them regularly throughout the project lifecycle to track ongoing compliance.

(3)	Determine the Required Identifying Information.	• It is good practice to begin planning and research with an assessment of the types of identifying information necessary to achieve the project's objectives.
		  ○ This can be done by outlining what information will be collected, who will access it, and how it will be stored and disclosed.
		  ○ Agency privacy officers should be able to articulate the business purpose for the identifying information collected or disclosed.

(4)	Analyze the Identifying Information's Contextual Integrity.	• The privacy by design approach calls for conducting a thorough analysis of the identifying information's contextual integrity and the current privacy landscape related to the project.
		  ○ This should include reviewing the project against the City's Privacy Principles and relevant laws, regulations, and contracts, as well as researching related pre-existing projects and technologies to evaluate past lessons learned.
		  ○ This analysis provides foundational context for privacy decisions throughout the project.

(5)	Implement Appropriate Privacy-Enhancing Techniques and Technologies.	• Based on results from the previous steps of analysis, select privacy-enhancing techniques and technologies. These should provide an appropriate level of privacy protection tailored to the project's specific context. ○ Consult with technical and staff to ensure these are properly implemented before the project launches. ○ Consult with agency cybersecurity staff to integrate security practices into the design process and comply with citywide cybersecurity requirement. This includes discussing regular baselining of access rights and adhering to the principle of least privilege.
(6)	Implement Privacy by Default.	• Check that the systems and processes are configured to collect, disclose, and retain the minimum amount of identifying information required for the project's purpose. They should also provide users with privacy protection and decision-making capabilities appropriate to the project's context. ○ For example, users should have the ability to opt-in to non-essential features rather than having them enabled by default. ○ Privacy-enhancing techniques and technologies should provide an appropriate level of privacy protection tailored to the project's specific context.
(7)	Embed Privacy in the Business Case.	• Privacy considerations should be integral to the project's business case in requests for funding, presentations to management, and oversight reporting. ○ This can include highlighting privacy benefits such as reducing the risk of security incidents, enhancing public trust, and promoting regulatory and contractual compliance. ○ Select and highlight privacy-specific key performance indicators that could track the effectiveness of privacy controls and measure project success.

Privacy Impact Assessment

Overview

Completing this Privacy Impact Assessment supports agency privacy officers' analysis and integration of privacy considerations into the information handling and risk management aspects of their operations. By completing a privacy impact assessment early in the project development process, agency privacy officers can identify potential privacy issues early.

Privacy Impact Assessment Table of Contents

Instructions

Agency privacy officers should collaborate with relevant agency personnel to conduct a privacy impact assessment before implementing a new project that changes how the agency collects, uses, or discloses identifying information. A project may undergo substantive changes during its development, implementation, or post-deployment phases. If there are changes to the ways the identifying information is or will be collected, used, or disclosed, agency privacy officers should prepare a revised privacy impact assessment that references the original assessment and highlights the changes from the prior Privacy Impact Assessment.

If multiple agencies are involved in a single project, the participating agencies should work together to determine whether a single coordinated privacy impact assessment will be conducted by a "lead" agency or each agency will complete its own privacy impact assessment.

The privacy impact assessment should be understandable by a member of the public. Use plain English, define acronyms the first time you use them and, to the extent possible, define any technical terminology.

Contact Information

Instructions

Identify the agencies and individuals for each role identified below. An agency or individual may be listed more than once, depending on their role. Add rows to identify other meaningful roles and contacts.

If multiple agencies are involved in a single project, identify the agency that is primarily responsible for making operational decisions about the project as the lead agency.

Role	Identification	Contact information
Lead agency		
Other participating agencies (if any)		
Participating non-City entities (if any)		
Agency privacy officers		
Project owner within the lead agency (individual)		

Project Description

Name and non-technical description of the project, including the expected benefits of the project.

Basis for the Privacy Impact Assessment
This assessment involves (*select all that apply)*: ☐ A new project that changes how the agency collects, uses, or discloses identifying information. ☐ A change to how a project collects, uses, or discloses identifying information. ☐ A new technology or process, including artificial intelligence, that can collect, use, or disclose identifying information.

Privacy Analysis

Instructions

In both design and implementation, agencies are required to incorporate the City's Privacy Principles into their projects (CPO Policies and Protocols § 2)

#	Privacy Principle	Description
1	Transparency	City agencies must clearly inform the public about how and why they collect, use, disclose, access, and retain identifying information, as well as give people the opportunity to make choices about their identifying information, when possible.
2	Public Trust	City agencies must collect identifying information lawfully and fairly and, when possible, directly from people with their knowledge and consent. Agencies should publicly share details about their privacy practices and handling of identifying information, where appropriate.
3	Accountability	City agencies must implement privacy practices, and periodically assess, audit, and modify them as necessary to keep pace with privacy and security threats and standards and best practices.
4	Data Minimization	City agencies must collect, use, disclose, access, and retain identifying information only as necessary for an articulated and legally permissible purpose and utilizing the minimum necessary data elements for the stated purpose.
5	Use Limitation	City agencies must articulate the specific need for each collection, use, disclosure, access to, or retention of identifying information, including the legal authority and agency purpose, and only use identifying information in ways compatible with the purpose of the collection.
6	Responsible Governance and Stewardship	City agencies must protect identifying information and should collect, use, disclose, access, and retain identifying information only through authorized persons for authorized purposes.
7	Data Quality, Integrity, and Accuracy	City agencies must protect the quality, integrity, and accuracy of identifying information and take reasonable steps to correct, update, or securely dispose of inaccurate or outdated identifying information. City agencies should allow individuals to access and correct their identifying information when appropriate, as well as consider the context in which data elements are collected, used, disclosed, accessed, and retained.

#	Privacy Principle	Description
8	Security Safeguards	City agencies must use appropriate physical and digital safeguards to protect identifying information from threats and from unauthorized collection, use, disclosure, access, and retention and follow current privacy and security best practices and standards.
9	Equity	City agencies must consider equity in privacy protection and discourage, mitigate, and protect against discrimination, misuse, and exploitation in the collection, use, disclosure, access to, or retention of identifying information.

The following questions help you consider these principles in the collection, use, or disclosure of identifying information. Please answer all questions using the menu provided. Please use the additional space provided **only** as instructed and if the menu options do not address your implementation or use case.

"Identifying information" means any information obtained by or on behalf of the City that may be used on its own or with other information to identify or locate an individual.[1] The Identifying Information Law has a partial list of types of identifying information and authorizes the Chief Privacy Officer to designate additional types of information. The list of types of identifying information is non-exhaustive. Agencies must protect any information that alone or in combination with other information could identify or locate an individual.

[1] *See* Admin. Code § 23-1201.

1) **What types of identifying information are collected for the project?** The list below is not intended as an exhaustive list: if the project implicates information that, in your judgment and based on the context of its handling you would consider identifying information, list it in the space provided.

Enumerated Types of Identifying Information:	
Personal Information ☐Name ☐Social Security number (full or last 4 digits)* ☐Taxpayer ID number (full or last 4 digits)*	**Work-Related Information** ☐Employer information ☐Employment address
Biometric Information ☐Fingerprints ☐Photographs ☐Height† ☐Weight† ☐Palm and handprints* ☐Retina and iris patterns* ☐Facial geometry* ☐Gait or movement patterns* ☐Voiceprints* ☐DNA sequences*	**Government Program Information** ☐Any scheduled appointments with any employee, contractor, or subcontractor ☐Any scheduled court appearances ☐Eligibility for or receipt of public assistance or City services ☐Income tax information ☐Motor vehicle information ☐Shelter address*
Contact Information ☐Current and/or previous home addresses ☐Email address ☐Phone number	**Health Information** ☐Mental or physical condition* ☐Prescriptions* ☐Diagnoses* ☐Medical history* ☐Healthcare policy number*

† Types of identifying information added by Local Law 61 of 2023.
* Types of identifying information designated by the Chief Privacy Officer.

Demographic Information ☐Country of origin ☐Date of birth* ☐Gender identity ☐Languages spoken ☐Marital or partnership status ☐Nationality ☐Race ☐Religion ☐Sexual orientation	**Public Safety** ☐Arrest record or criminal conviction ☐Case identifiers* ☐Case disposition* ☐Date or time of release from custody ☐Information obtained from any surveillance system operated by, for the benefit of, or at the direction of the NYPD
Status Information ☐Citizenship or immigration status ☐Employment status ☐Status as victim of domestic violence or sexual assault ☐Status as crime victim or witness	**Technology-Related Information** ☐Device identifier including media access control (MAC) address or Internet mobile equipment identity (IMEI)* ☐GPS-based location obtained or derived from a device that can be used to track or locate an individual* ☐Internet protocol (IP) address* ☐Social media account information

* Types of Identifying Information designated by the Chief Privacy Officer.

2) **What types of identifying information are used for the project?** The list below is not intended as an exhaustive list: if the project implicates information that, in your judgment and based on the context of its handling you would consider identifying information, list it in the space provided.

Enumerated Types of Identifying Information:	
Personal Information ☐Name ☐Social Security number (full or last 4 digits)* ☐Taxpayer ID number (full or last 4 digits)*	**Work-Related Information** ☐Employer information ☐Employment address
Biometric Information ☐Fingerprints ☐Photographs ☐Height† ☐Weight† ☐Palm and handprints* ☐Retina and iris patterns* ☐Facial geometry* ☐Gait or movement patterns* ☐Voiceprints* ☐DNA sequences*	**Government Program Information** ☐Any scheduled appointments with any employee, contractor, or subcontractor ☐Any scheduled court appearances ☐Eligibility for or receipt of public assistance or City services ☐Income tax information ☐Motor vehicle information ☐Shelter address*
Contact Information ☐Current and/or previous home addresses ☐Email address ☐Phone number	**Health Information** ☐Mental or physical condition* ☐Prescriptions* ☐Diagnoses* ☐Medical history* ☐Healthcare policy number*

† Types of identifying information added by Local Law 61 of 2023.
* Types of identifying information designated by the Chief Privacy Officer.

Demographic Information ☐Country of origin ☐Date of birth* ☐Gender identity ☐Languages spoken ☐Marital or partnership status ☐Nationality ☐Race ☐Religion ☐Sexual orientation	**Public Safety** ☐Arrest record or criminal conviction ☐Case identifiers* ☐Case disposition* ☐Date or time of release from custody ☐Information obtained from any surveillance system operated by, for the benefit of, or at the direction of the NYPD
Status Information ☐Citizenship or immigration status ☐Employment status ☐Status as victim of domestic violence or sexual assault ☐Status as crime victim or witness	**Technology-Related Information** ☐Device identifier including media access control (MAC) address or Internet mobile equipment identity (IMEI)* ☐GPS-based location obtained or derived from a device that can be used to track or locate an individual* ☐Internet protocol (IP) address* ☐Social media account information

* Types of Identifying Information designated by the Chief Privacy Officer.

3) **What types of identifying information are disclosed for the project?** The list below is not intended as an exhaustive list: if the project implicates information that, in your judgment and based on the context of its handling you would consider identifying information, list it in the space provided.

Enumerated Types of Identifying Information:	
Personal Information ☐Name ☐Social Security number (full or last 4 digits)* ☐Taxpayer ID number (full or last 4 digits)*	**Work-Related Information** ☐Employer information ☐Employment address
Biometric Information ☐Fingerprints ☐Photographs ☐Height† ☐Weight† ☐Palm and handprints* ☐Retina and iris patterns* ☐Facial geometry* ☐Gait or movement patterns* ☐Voiceprints* ☐DNA sequences*	**Government Program Information** ☐Any scheduled appointments with any employee, contractor, or subcontractor ☐Any scheduled court appearances ☐Eligibility for or receipt of public assistance or City services ☐Income tax information ☐Motor vehicle information ☐Shelter address*
Contact Information ☐Current and/or previous home addresses ☐Email address ☐Phone number	**Health Information** ☐Mental or physical condition* ☐Prescriptions* ☐Diagnoses* ☐Medical history* ☐Healthcare policy number*

† Types of identifying information added by Local Law 61 of 2023.
* Types of identifying information designated by the Chief Privacy Officer.

Demographic Information ☐Country of origin ☐Date of birth* ☐Gender identity ☐Languages spoken ☐Marital or partnership status ☐Nationality ☐Race ☐Religion ☐Sexual orientation	**Public Safety** ☐Arrest record or criminal conviction ☐Case identifiers* ☐Case disposition* ☐Date or time of release from custody ☐Information obtained from any surveillance system operated by, for the benefit of, or at the direction of the NYPD
Status Information ☐Citizenship or immigration status ☐Employment status ☐Status as victim of domestic violence or sexual assault ☐Status as crime victim or witness	**Technology-Related Information** ☐Device identifier including media access control (MAC) address or Internet mobile equipment identity (IMEI)* ☐GPS-based location obtained or derived from a device that can be used to track or locate an individual* ☐Internet protocol (IP) address* ☐Social media account information

* Types of Identifying Information designated by the Chief Privacy Officer.

4) **What are the sources of the identifying information collected as part of the project?** If the identifying information is from more than one source, indicate all sources and the kinds of information obtained. If the project does not involve the collection of identifying information, mark "N/A" in the space below.

☐ Direct from individual ☐ Another City agency ☐ Another government entity (local/State/Federal/non-US)	☐ Non-government entity (explain in space provided) ☐ Other (explain in space provided) ☐ N/A
(If "non-government entity" or "other," please explain. If the identifying information is from a commercial source, identify the vendor and explain why use of a commercial data source is necessary.)	

5) **What are the sources of the identifying information used as part of this project?** If the identifying information is from more than one source, indicate all sources and the kinds of information obtained. If the project does not involve the use of identifying information, mark "N/A" in the space below.

☐ Direct from individual ☐ Another City agency ☐ Another government entity	☐ Non-government entity (explain in space provided) ☐ Other (explain in space provided) ☐ N/A
(If "non-government entity" or "other," please explain. If the identifying information is from a commercial source, identify the vendor and explain why use of a commercial data source is necessary.)	

6) **What are the sources of the identifying information disclosed as part of this project?** If the identifying information is from more than one source, indicate all sources and the kinds of information obtained. If the project does not involve the disclosure of identifying information, mark "N/A" in the space below.

☐ Direct from individual ☐ Another City agency ☐ Another government entity (local/State/Federal/non-US)	☐ Non-government entity (explain in space provided) ☐ Other (explain in space provided) ☐ N/A
(If "non-government entity" or "other," please explain. If the identifying information is from a commercial source, identify the vendor and explain why use of a commercial data source is necessary.)	

7) **List all recipients of identifying information that will be collected, used, or disclosed during the project.** If multiple parties are participating in the project, indicate whether a data-sharing agreement is or will be put in place prior to the collection, use, or disclosure of information.

(List each recipient (such as the agency, division, contractor, individuals, etc.) and what types of identifying information they will receive. Indicate whether there will be an applicable data-sharing agreement. If there will be no agreement, explain.)

8) **Is any identifying information disclosed to non-City third parties?** If the project involves AI Systems developed and maintained by a vendor, could identifying information be used by a vendor for further training or development of the AI Systems?

☐ YES (explain in space provided)	☐ NO
(If "YES," please explain)	

9) **If any identifying information is being disclosed as part of the project (whether to another City entity or a non-City third party), is the recipient required to notify the disclosing agency (or anyone else) prior to re-disclosing the identifying information to another party?**

☐ YES	☐ NO (explain in space provided)
(If "NO," please explain)	

10) Is identifying information being collected, used, or disclosed with consent or without consent?

☐ WITH CONSENT	☐ WITHOUT CONSENT (explain in space provided)
(If WITHOUT CONSENT, please explain)	

Legal Authorities

1. **Does the project involve more than one agency?**

☐ YES (explain in space provided)	☐ NO
(If "YES," please describe whether data-sharing agreements are required and describe all inter-agency agreements governing the handling of the identifying information)	

2. **Does the project involve any non-City entity?**

☐ YES (explain in space provided)	☐ NO
(If "YES," please describe any contracts or other documentation governing the handling of the identifying information)	

3. **What laws, regulations, or compliance frameworks govern the information being collected, used, or disclosed?** If the identifying information is governed by more than one regulatory framework (such as a project involving multiple agencies), indicate all applicable frameworks.

(Indicate applicable frameworks)

4. **What is the agency's legal basis for the collection, use, or disclosure of the identifying information?**

(Provide all applicable statutory citations)

5. **Does the agency require legal approval from any other entity to disclose or use identifying information for the project?**

☐ YES (explain in space provided)	☐ NO
(If "YES," please explain)	

Technical details

1. **What is the security classification of the identifying information used as part of the project?** Reference the Citywide Data Classification Policy and Citywide Data Classification Standard.

   ☐Restricted ☐Sensitive

2. **Where is the identifying information stored by the recipient of the disclosed information?**

☐Agency servers ☐Other government servers ☐Agency-issued mobile devices	☐"Bring your own" devices ☐Hard copies ☐Cloud provider (explain in space provided) ☐Other (explain in space provided

3. **If the agency is using a cloud provider, detail whether the agency has completed cloud review and all required contract processes.** If the agency is using a storage method not listed, use the space below to explain.

4. **What *administrative* controls are or will be used to govern the handling of identifying information?** Examples of administrative controls might include data classification policies, acceptable use policies, and non-disclosure agreements. If different administrative controls are or will be implemented to safeguard different kinds of identifying information, describe all administrative controls to be used.

5. **What *physical* access controls are or will be used to restrict access to identifying information to authorized parties?** If different physical controls are or will be implemented to safeguard different kinds of identifying information, describe all physical controls to be used.

☐Secured location with controlled access ☐Locked safe ☐Surveillance	☐Other (explain in space provided) ☐None (explain in space provided)
(If "Other" or "None," please explain)	

6. **What *technical* controls are or will be implemented to protect identifying information from unauthorized access?** If different technical controls are or will be implemented to safeguard different kinds of identifying information, describe all technical controls to be used.

☐Encryption of data at rest ☐Encryption of data in transit ☐Firewall ☐Privileged access/IAM	☐Intrusion detection system ☐Other (explain in space provided) ☐None (explain in space provided)
(If "Other" or "None," please explain)	

Retention and disposal

1. **Will the identifying information be destroyed upon completion of the project?**

☐ YES	☐ NO
(If "NO," please explain)	

2. **Is the retention period consistent with the agency's retention policy?**

☐ YES	☐ NO (explain in space provided)
(If "NO," please explain)	

3. **Will recipients destroy the identifying information upon completion of the project?**

☐ YES	☐ NO (explain in space provided)
(If "NO," please explain)	

4. How will the recipient dispose of identifying information used or disclosed for the project?

☐Shredding ☐Degaussing identifying information ☐2/3X overwriting	☐Deletion ☐Other (explain in space provided)
(If "other," please explain)	

Risk and mitigation

1. **Does the project minimize the amount and types of identifying information collected, used, or disclosed, considering the project's purpose?**

☐ YES	☐ NO (explain in space provided)
(If "NO," please explain)	

2. Refer to the project description at the beginning of this Privacy Impact Assessment. **Based on the description, the types of identifying information involved in this project, and the flow of data, list the potential risks to the privacy and security of the identifying information arising from the project.**

3. **Describe in detail how each of the risks identified above will be mitigated**.

APO Certification:

I have reviewed this document, which reflects my understanding of the project.

_____

APO Signature and Date

_____

Print Name

Guidance for Drafting Program-Specific Privacy Policies

Instructions

Agencies may use this document to write program-specific privacy policies for their programs, services, products, or other initiatives. The sample language is meant to highlight the basic components and common issues that could be covered in such privacy policies. It is not intended to enumerate all the issues that should be covered, nor is it intended to suggest that all the issues should be covered. Agency privacy officers should customize the sample language as appropriate for the specific use case. This includes choosing relevant sample language, adding more language, modifying the legal substance, and modifying the writing style to make the language understandable to and appropriate for the subject and audience. The final policy should accurately represent the agency's actual practices regarding the information covered by the policy.

When creating program-specific privacy policies, agency privacy officers should consult with agency counsel.

Introductory paragraph.

This privacy policy describes how the City of New York through [insert agency name] collects, stores, uses, and shares information when you use [insert name] (**this Service**).

How and why do we collect information?

[Option] We collect information to further legitimate governmental purposes.

[Option] We collect this information to further legitimate governmental purposes. Specifically, [insert specific purposes].

What information do we collect from you?

[Option] We collect the information you provide to us. We also automatically collect [insert all other information you collect, or general categories: e.g., IP address or proxy server, internet service provider, or mobile carrier, device information, browser type and settings, application id number, date/time stamps associated with your usage, pages and files viewed, searches, system configuration information, system activity, system error reports].

[Option] We do not collect information about your location.

[Option] We collect information about your location. We collect this information because [insert reason].

[Option] You can opt out of allowing us to collect this information either by refusing access to the information or by disabling your location setting on your device. However, if you choose to opt out, you may not be able to use certain aspects of this Service.

Do we use cookies or similar technologies?
Yes. This Service uses cookies or similar technologies to [insert reasons such as: provide a good user experience, enable interactive content, enable analytics, etc.]. See the Cookies Policy for more information.

No. This Service does not use cookies or similar technologies.

Who should NOT use this Service?

[Option] Children under 13 years old should not use this Service.

[Option] Children under 18 years old should not use this Service.

What do we do with your information?

[Option] We use your information to [insert details of use]**.**

[Option] We do not share your information without your explicit permission.

[Option] We may share your information with City or other government agencies for [reason].

[Option] We may share your answers with nonprofits and other partners for [reason].

[Option] We use your information to produce aggregate data to [insert reason]**.** Your identifying information or individual answers will not be included in any aggregate reports.

[Option] We may combine your information with any other information we already have about you.

[Option] We do not combine your information with any other information we already have about you.

[Option] Information that could be used to identify you will not be shared with any private party except as required by a court of competent jurisdiction.

When and with whom do we share your information?

[Option] There are no specific limits on how we share your information, but we will comply with all applicable laws.

[Option] We share information when [insert when] and with [insert with whom].

Whether we will combine information you give us information with information from other sources?

[Option] We will not combine information you give us with information from other sources.

[Option] We will combine information you give us with information from other New York City agencies, but not with information from other sources.

[Option] We will combine information you give us with information from other governments, but not with information from other sources.

[Option] We will combine information you give us with information from [insert sources].

Do we use your information for commercial purposes?
[Option] No. We do not rent, sell, or otherwise use your information for commercial purposes, nor for external marketing purposes.

How do we keep your information safe?

[Option] We use organizational and technical processes and procedures to protect your information.

[Option] However, because no electronic communication can be 100% secure, we cannot guarantee that unauthorized parties can gain unauthorized access to your information.

[Option] To protect your information, we use [insert organizational and technical processes and procedures].

How long do we keep your information?

[Option] We keep your information for as long as necessary to fulfill the purposes outlined in this privacy policy unless otherwise required by law.

[Option] We keep your information for [insert the amount of time] unless otherwise required by law.

Will you contact me after I start using this Service?

[Option] Yes. We may contact you about [insert circumstances].

[Option] However, you may opt-out of further contact by withdrawing your consent pursuant to [insert reference to withdrawal of consent section]**.**

[Option] Yes, but only for purposes of [insert purposes]**.**

[Option] However, you may opt-out of further contact by withdrawing your consent pursuant to [insert reference to withdrawal of consent section]**.**

[Option] No. We will not contact you for any reason unless you opt-in by [insert opt-in method]**.**

How can you withdraw your consent to use the information we collect from you?

[Option] You may withdraw your consent for us to use the information we collect. You may do so at any time by emailing us at [insert email address]**.**

[Option] You may withdraw your consent for us to use or disclose new information we collect from you, but we may continue to use information that we have already collected from you.

[Option] You cannot withdraw your consent for using the information we collect.

How can you review, update, or delete your information?

[Option] To request to review, update, or delete your information, please contact us at [insert email address].

[Option] You cannot review, update, or delete your information after it is collected.

How can you ask questions about this Service?

[Option] You can ask questions about this Service by [insert contact method and details].

Will your use of the Service affect any benefits you receive?

[Option] No. Use of this Service will not affect any New York City-provided benefits you receive.

[Option] Yes. This Service could affect your current New York City provided benefits. [insert how; e.g., Service allows you to apply for benefits, or to provide information that may be used to reassess qualification for benefits or to reassess the level of benefits you receive].

How do we handle illegal activities?

We fully cooperate with law enforcement agencies in identifying those who may try to access services for illegal activities. We reserve the right to report to law enforcement agencies any activities that we, in good faith, believe may be unlawful.

Guidance on Selecting Privacy-Enhancing Techniques and Technologies

Instructions

This section provides guidance regarding approaches for selecting privacy-enhancing techniques and technologies. While privacy-enhancing techniques and technologies may increase privacy protection, some may result in unintended consequences such as the loss of data accuracy, increased computing costs, and the amplification of biases. This document provides descriptions of several privacy-enhancing techniques and technologies and associated considerations that may accompany their use but does not provide instructions for technical implementation. Consult with the Office of Information Privacy for assistance when considering privacy-enhancing techniques and technologies in specific circumstances. Completing or referencing the Privacy Impact Assessment in the Agency Privacy Officer Toolkit can also help agencies choose the proper privacy-enhancing technique or technology commensurate to the specific privacy risks.

Summary of Privacy Enhancing Techniques and Technologies			
Method	**Trigger**	**Description**	**Risks**
Aggregation	Sharing reports, statistics, or research.	Compiling data into summaries to de-identify individuals (e.g., reporting how many people applied from a borough).	Risk of over-generalization, potential for re-identification, reduced data usefulness.
Suppression	Sharing public reports where small groups might be re-identified.	Replacing data related to small numbers with a placeholder (e.g., if three public benefit recipients reside at the same address, an agency can replace "3" with "*" to denote the recipients.	Limited accuracy for small datasets, possible information loss, potential for re-identification.
Pseudonymization	Masking personal information in datasets to prevent re-identification.	Substituting identifying data with non-identifying labels (e.g., replacing a name with "A.").	Re-identification risks if other identifying information remains, reduced data usefulness.
Redaction	Sharing or publishing documents containing identifying information.	Removing identifying information from documents (e.g., deleting birthdates).	Ensuring complete and irreversible removal of sensitive data.
Differential Privacy	Sharing statistical data while strengthening privacy protection.	Adding statistical noise to original data to illustrate group patterns while reducing the risk of identifying individuals in summary statistics (e.g. census data).	Appropriate balance between privacy strength and analytic accuracy, known as the privacy budget, may be difficult to determine. Currently, there is not a widely accepted method to determine the appropriate privacy budget for a given use case. Potential to amplify biases.

Summary of Privacy Enhancing Techniques and Technologies			
Method	**Trigger**	**Description**	**Risks**
Synthetic Data	Conducting data sharing or analysis while needing to preserve confidentiality.	Generating artificial data points that mimic real-world data patterns (e.g. for sandbox testing, sharing certain data with vendors, training machine learning models).	Potential leakage of sensitive information from the original dataset if not carefully handled, potential to amplify biases, potential data quality issues. Risk of distorting key statistical features of the original data distribution if not modeled properly.
Homomorphic Encryption	Conducting data analysis while needing to preserve confidentiality of a data source from the party seeking to do analysis.	Performing computations on encrypted data without having access to the underlying unencrypted data.	High computation costs and limited independent practical applications.
Secure Multiparty Computation	Enabling collaborative analysis on multiple data sources while needing to preserve confidentiality of the underlying data.	Performing computations jointly across multiple parties' datasets while limiting the risk of identification.	High computation costs and limited independent practical applications.
Private Set Intersection	Determining common records or clients while limiting the disclosure of identifying information.	Identifying overlapping records across datasets while limiting leakage of non-matching data.	High resource requirements for large datasets, potential data quality issues from sources of origin may cause performance issues.
Zero – Knowledge Proofs	Proving a person's identity and/or eligibility without disclosing identifying information.	Mathematically proving parties' possession of certain attributes without exposing underlying data.	High computational costs and difficulty integrating with traditional systems. Difficulty of validating the result apart from replicating the computation.

Summary of Privacy Enhancing Techniques and Technologies			
Method	**Trigger**	**Description**	**Risks**
Federated Learning	Building an AI model with multiple parties' data without sharing underlying data.	Training local models separately on parties' data and then integrate the results into the larger model.	Privacy risks related to machine learning apply. Includes potential for reconstructing the original training data or identifying if a given sample is from the original dataset.

Guidance for Assessing Contextual Integrity

Addressing contextual integrity[2] requires agencies, with the guidance and involvement of their agency privacy officers, to methodically balance data collection, disclosure, and retention with privacy expectations, operational goals, and legal requirements. This process involves several critical steps that align program operations to respect individual privacy and maintain trust.

Define the Context and Sub-Contexts. The first step is to establish the program's context and any relevant sub-contexts. For example, a program offering shelter services might fall under the broader umbrella of social services. Within this context, specific sub-contexts may emerge, such as health care, financial services, or employment. Each sub-context carries unique privacy expectations and regulatory requirements.

Understanding sub-contexts allows agency privacy officers to focus on the distinct nuances of each. For instance, healthcare contexts often necessitate strict confidentiality, while financial services might require heightened security for transactional data. By delineating these areas, agency privacy officers, in collaboration with appropriate agency staff, can tailor data-handling practices to compliance needs and operational feasibility, setting privacy levels that match the specific demands of each sub-context.

Evaluate Laws, Expectations, and Past Practices. With the defined context, agency privacy officers should evaluate the regulatory environment, privacy norms, and historical precedents. Agency privacy officers, in consultation with agency counsel, should identify the laws and regulations applicable to the program and should require that practices adhere to the appropriate legal frameworks. At the same time, agency privacy officers should understand the privacy expectations of individuals, recognizing that these expectations may differ depending on the sub-context. For instance, beneficiaries of health care services may expect more stringent privacy protections than those participating in financial assistance programs. Similarly, the social backdrop of a community event may cause attendees to expect different privacy protections than does a meeting with a tax preparation service.

Building on this foundation, agency privacy officers, in collaboration with appropriate agency staff, should analyze past practices in similar circumstances. They should assess what worked effectively in the past, identify past challenges, and use these insights to refine their approach. This combination of legal compliance, privacy alignment, and historical insight helps agencies limit data collection, retention, and disclosure to what is justified and operationally necessary, and always tied to a clear and articulated purpose.

Map the Actors and Define Roles. Identifying the actors involved in a program is a crucial step in managing contextual integrity. Agency privacy officers should map out all participants, including individuals, such as applicants and program staff, and entities, such as other city agencies or contractors. In collaboration with appropriate agency staff, agency privacy officers should identify roles so that that only those with a legitimate need access identifying information. For example, in a program involving contractors, agency privacy officers can identify specific individuals within the contractor organization who require access so that their access to identifying information is appropriately restricted and their permitted use is clearly defined.

The process may also involve securing informed consent from individuals for data collection and disclosure, establishing clear data-sharing agreements between participating entities, and creating well-defined

[2] See CPO Policies and Protocols Sections 3.2.8 and 4.3.

responsibilities. Agency privacy officers should consider how information is collected, disclosed, retained, and processed, identifying who will handle each step and providing accountability in case of an unauthorized collection, use, or disclosure.

Categorize and Protect Data Attributes. To maintain contextual integrity, agency privacy officers should evaluate the types of data collected to align with the program's objectives. They should focus on collecting only what is necessary and relevant while avoiding overly detailed or sensitive attributes that could increase privacy risks. For example, in a traffic study aimed at improving intersection safety, general data on road users may suffice, while granular personal details about individual drivers are both unnecessary and potentially risky.

Agency privacy officers, with the assistance of appropriate agency staff, should also assess the reliability of the data, excluding information that may be inaccurate or introduce errors into the analysis. By narrowing the focus to essential data attributes and applying protections to sensitive categories, agency privacy officers balance the need for actionable insights with the imperative to safeguard individual privacy.

Establish Transmission Principles. When identifying information is disclosed, agency privacy officers should review its transmission methods to align with the program's purpose and respects individual privacy expectations. They should verify that routing practices comply with privacy policies and operational goals and that, if appropriate, individuals are aware of and consent to how their identifying information will be used. Transparency is key, as it fosters trust between the agency and the people it serves.

Transmission methods should be appropriately secure, with safeguards proportional to the sensitivity of the data. If contractors handle data during the process, agency privacy officers may impose legal and operational requirements so that these entities uphold privacy standards.

By following these steps, agencies and agency privacy officers can effectively operationalize contextual integrity, balancing program objectives with respect for individual privacy and compliance with legal standards. This structured approach enhances trust, transparency, and accountability in the management of identifying information.

Best Interests of the City Determination Request Instructions			
Instructions to request approval from the Chief Privacy Officer to deviate from the standard text of the Identifying Information Rider language.			
	Task	**Description**	**Reference**
(1)	Complete Best Interests of the City Determination Form	Open Best Interests of the City Determination Request Form	☐
(2)	Question 1: Name of the city agency making the request: *if "other" is selected, please provide the name of the city agency	**Select** your agency that you are submitting the determination for. ***Type** into the box (next to other) the **FULL NAME** of the agency requesting the deviation.	☐
(3)	Question 2: Specify whether the request is for a collection, a disclosure, or both:	Select **1** option from the given answers: 1. *Collection* 2. *Disclosure* 3. *Both*	☐
(4)	Question 3: Describe the identifying information that will be collected and/or disclosed:	**Type** your answer to the question into the box.	☐
(5)	Question 4: Describe the purpose of collecting and/or disclosing the identifying information:	**Type** your answer to the question into the box.	☐
(6)	Question 5: Describe the source of the identifying information:	**Type** your answer to the question into the box.	☐
(7)	Question 6: Describe the recipient of the identifying information:	**Type** your answer to the question into the box.	☐
(8)	Question 7: Identify other city agencies interested in this collection and/or disclosure:	**Type** the full names of the agencies interested in the collection or disclosure.	☐
(9)	Question 8: Explain why this collection and/or disclosure is not required by law or treaty:	**Type** your answer to the question into the box.	☐
(10)	Question 9: Explain why this collection or disclosure does not further the mission or purpose of the agency:	**Type** your answer to the question into the box.	☐

Best Interests of the City Determination Request Instructions			
Instructions to request approval from the Chief Privacy Officer to deviate from the standard text of the Identifying Information Rider language.			
	Task	**Description**	**Reference**
(11)	Question 10: Explain why you believe this collection or disclosure is in the best interests of the City:	**Type** your answer to the question into the box.	☐
(12)	Question 11: Specify the start date and duration of the collection or disclosure:	**Type** your answer to the question in MM/DD/YYYY.	☐
(13)	Submitter Information and Verification	**Type** and **Select** proper information.	☐

Identifying Information Rider Deviation Request Instructions			
Instructions to request approval from the Chief Privacy Officer to deviate from the standard text of the Identifying Information Rider.			
	Task	**Description**	**Reference**
(1)	Complete Identifying Information Rider Deviation Worksheet	Open Identifying Information Rider Deviation Request Form	☐
(2)	Question 1: Name of the city agency making the request: *if "other" is selected, please provide the name of the city agency	**Select** the agency name from drop down options; if the agency name is not listed, select "other." **Type** into the box (next to other) the **FULL NAME** of the agency requesting the deviation.	☐
(3)	Question 2: Why do you believe that the Identifying Information Rider is required for this contract?	Select all options that apply: 1. *Contracts and subcontracts for human services (CPO Policies 6.1.1).* 2. *Contracts and Subcontracts for Technology Services Involving Sensitive Identifying Information (CPO Policies 6.1.2.1).* 3. *Contracts and Subcontracts for Outreach Services Involving Identifying Information (CPO Policies 6.1.2.2).*	☐
(4)	Question 3: Describe the contract (purpose, parties, terms) and any special or unique provisions other than privacy clauses themselves:	**Type** your answer to the question into the box.	☐
(5)	Question 4: Specify the data elements that will be collected, used, or disclosed by the contractor:	**Type** your answer to the question into the box.	☐
(6)	Question 5: Identify other city agencies interested in this collection and/or disclosure:	**Type** your answer to the question into the box.	☐
(7)	Question 6: Upload Requested Deviations Worksheet:	Upload completed worksheet. The worksheet identifies and justifies the specific deviations being requested. Requested Deviations Worksheet	☐

Identifying Information Rider Deviation Request Instructions			
Instructions to request approval from the Chief Privacy Officer to deviate from the standard text of the Identifying Information Rider.			
	Task	**Description**	**Reference**
(8)	Question 7: Describe any similar deviations from the standard text of the Identifying Information Rider your agency has agreed to in the past. Include a description of the specific contract containing the provisions and parties to the contract:	**Type** your answer to the question into the box. For example, identify other contracts that incorporated the requested deviations.	☐
(9)	Question 8: Is this artificial intelligence related?	Select **1** option from the given answers: 1. *Yes* 2. *No*	☐
(10)	Question 9: Explain why you believe this collection or disclosure is in the best interests of the City:	**Type** your answer to the question into the box.	☐
(11)	Question 10: Upload current draft of the agreement:	Upload **current draft** from computer	☐
(12)	Submitter Information and Verification	**Type** and **Select** proper information.	☐

Guidance Related to Terms Under the Identifying Information Rider and Privacy Protection Rider

Instructions

The Identifying Information Rider Section 8.0 and Privacy Protection Rider Section 8.0 require contractors to provide reports to the agency privacy relating to the contractors' collections, retentions, disclosures, and uses of identifying information. The material below is intended to assist agency privacy officers compose questions and other information requests for their contractors. Some areas of questioning may be suitable when engaging a contractor, others as routine mid-contract maintenance, and others when the agency privacy officer has reason to suspect that a contractor is not complying with the contract terms. Agency privacy officers should adopt question areas and forms that are suitable for the circumstances and should engage other agency stakeholders when developing their information requests.

The material below also includes guidance with questions and sample provisions to help agencies draft contract provisions to protect sensitive identifying information for contracts that are not "covered contracts" as such term is defined in the Citywide Privacy Protection Policies and Protocols.

Questions Relating to the Contractor's Internal Processes:

- Are you currently compliant with the privacy obligations outlined in your agreement with the agency? If not, describe each area of noncompliance and, for each area, any corrective actions you are taking to become compliant.
- Have there been any changes to your privacy policies since the agreement was executed? If so, please provide a summary or attach the revised policies.
- Identify the person and office currently responsible for overseeing compliance with the privacy obligation in the agreement. Include name, title, and contact information.
- Have all employees with access to identifying information under the agreement completed privacy training? Provide a summary of the training, rates of compliance, and an overview of completion dates.
- Have you conducted any privacy risk assessments (or the like) since the agreement was executed? If so, provide a summary of the findings.
- Have you tested your capacity to comply with your obligations under the agreement (such as the procedure to follow for requests for identifying information, notifying the agency of a potential violation of the Identifying Information Rider, or a request from the agency to destroy identifying information)? If so, describe the test.

Questions to ask about the Contractor's Compliance with Laws and Regulations:

- Have there been any changes in privacy laws or regulations that impact your obligations under the agreement? If so, describe the changes and how you have responded to them.
- Please list all privacy laws and regulations that apply to your obligations under the agreement.

- Have you been the subject of any privacy-related investigations or complaints since the execution of the agreement? If so, provide details, including the nature of the investigations or complaints, the current status, and any corrective measures you have taken in response.

Questions to ask about the Contractor's Collections, Uses, and Disclosures of Identifying Information.

- Have you approved any collections or disclosures of identifying information since the agreement was executed?
- Have you considered, but not requested, that the agency approve collections or disclosures since the agreement was executed? Explain why.
- List all types of identifying information you are collecting and disclosing under the agreement. Explain if the list has changed since the agreement was executed.
- Have you received any requests for the identifying information under the agreement? Please list all requests, the date you received them, their current status, and whether and what types of identifying information you disclosed.

Questions to ask Related to Subcontractors.

- Have you engaged any subcontractors to fulfill your obligations under the agreement? Please list the subcontractors, their roles, and your process for vetting, approving, and supervising their compliance with the agreement.
- Have any subcontractors been out of compliance with the agreement? If so, identify the subcontractor, the details of the noncompliance, and your response.

Guidance for Drafting Contract Privacy Terms to Protect Sensitive Identifying Information

The questions and sample provisions below are provided to help agencies draft contract provisions to protect sensitive identifying information for contracts that are not "covered contracts" as such term is defined in the Citywide Privacy Protection Policies and Protocols.

1. Granting Non-City Entities Permission to Collect, Use, Disclose, or Access Sensitive Identifying Information

Question: Will the contractor or subcontractor collect, use, disclose, or access any sensitive identifying information?

Guidance: If so, include provisions that specifically identify the information, at the data element level, to be treated as "sensitive" (and include the definition of "Sensitive Identifying Information" provided in this Policy). Agencies should also specify which individual users (or groups of users) will be permitted to access the sensitive identifying information, and the specific purpose for which access is permitted. The provisions should specify the degree of care[3] and the measures that those with access should use when handling or accessing the Sensitive Identifying Information.

In addition, if the agreement does not include Office of Technology and Innovation's Attachment SCY, it should include protocols that explain how to handle suspected or known data incidents resulting in the unauthorized disclosure of Sensitive Identifying Information or other confidential information, such as a data security "breach" or any mishandling of information that violates the Identifying Information Law. Contractors and subcontractors should be required to cooperate with City agencies in investigating and handling such incidents. The agreement provisions should also include required timeframes for notifying other parties, including: notifying affected individuals where required by law; requiring mitigation efforts to prevent or minimize any harm that could result from such incidents; and safeguards against re-disclosure.

Sample language: Contractor shall hold all Confidential Information, including Sensitive Identifying Information, in strict confidence. Contractor shall only use Confidential Information in the good-faith performance of its obligations under this Agreement. Contractor shall immediately notify Agency in writing upon discovery of any actual or suspected improper use or disclosure of Confidential Information (**Improper Use or Disclosure**), which shall include, without limitation, any improper collection, use, disclosure of, or access to Confidential Information other than as authorized by this Agreement or applicable law. In the event that Contractor discovers or suspects any improper use or disclosure of any Confidential Information, Contractor shall promptly, but no later than 24 hours of such incident, notify Agency of same, and shall take all reasonable steps to mitigate the impact of such

[3] Typical standards of care require a contractor or subcontractor to exercise at least the same degree of care that the contractor or subcontractor uses to preserve the confidentiality of its own information of similar character, but in any event, at least a reasonable degree of care.

Improper Use or Disclosure, and cooperate with Agency to investigate and prevent any further improper use or disclosure of Confidential Information. Improper Use or Disclosure of Confidential Information constitutes a breach of this Agreement and may lead to termination of this Agreement, among other remedies available in law or equity to Agency.

2. Prohibiting Third Parties from Collecting, Using, Disclosing, or Accessing Sensitive Identifying Information

Question: Does the agency want to prohibit the contractor from allowing third parties to collect, use, disclose, or otherwise access some or all Sensitive Identifying Information that is available to the contractor or its subcontractor through the City contract?

Guidance: The agreement should specify the type of Sensitive Identifying Information that the contractor must not disclose to third parties, as well as the circumstances when the contractor is authorized to disclose such information to any specific third parties.

Sample language: Notwithstanding the restrictions to disclosure set forth above, Contractor may disclose Sensitive Identifying Information as required by judicial order, lawfully issued subpoena, other order or notice of a court or administrative body of competent jurisdiction, or as otherwise required by law. If Contractor receives such a request, Contractor must provide written notice to Agency within five (5) business days of receiving the request, before disclosing Sensitive Identifying Information in response to the request, in order to permit Agency to seek an appropriate protective order or other legal relief. Contractor shall not otherwise disclose Sensitive Identifying Information to any third parties without the Agency's prior written authorization.

3. Authorizing Contractors or Subcontractors to Retain Sensitive Identifying Information

Question: Will the contractor or its subcontractors seek or need to retain any Sensitive Identifying Information?

Guidance: If so, the agreement should specify the length of time that the contractor may retain the Sensitive Identifying Information, and require that the contractor confidentially maintain such information unless disclosure is authorized by the contract or required by law. The agreement should state that the provisions relating to confidentiality will survive termination of the agreement. The agreement should also include terms that explain requirements for data destruction or return to the City, including any certification of destruction by contractor, or where such requirements are infeasible for providing written justification.

Sample language: Upon the termination of this agreement for any reason, Contractor shall return to Agency, or destroy (unless otherwise required by law), all Sensitive Identifying Information in any form that Agency disclosed to Contractor in connection with this Agreement, including copies and abstracts thereof, within thirty (30) days of termination. Contractor must confirm such data destruction in writing within sixty (60) days of this Agreement's termination, and provide a certificate of destruction where requested by Agency. If Contractor determines that

returning or destroying any or all of the Sensitive Identifying Information is infeasible, Contractor shall promptly provide to Agency written justification and an explanation of the conditions that make return or destruction infeasible. In such instance, Contractor shall extend the protections of this Agreement to all Sensitive Identifying Information for which return or destruction is infeasible, and shall limit further uses and disclosures of Sensitive Identifying Information to those purposes that make the return or destruction infeasible, for so long as Contractor maintains Sensitive Identifying Information.

4. Authorizing Contractors to Conduct Data Analysis involving Sensitive Identifying Information to Improve Agency Services, or Using De-Identified, Anonymized, Pseudonymized, or Aggregated Data Derived from Sensitive Identifying Information

Question: Has the contractor requested, and does the Agency wish to authorize, contractor's use of any sensitive identifying information provided or made available by the City through a contract, including any de-identified, anonymized, pseudonymized (assignment of random or artificial identifiers), or aggregated data derived from such sensitive identifying information, to conduct its own data analyses beyond the contracted purpose?

Guidance: If so, the agreement must expressly detail the specific type of Sensitive Identifying Information that the contractor proposes to analyze, including each data element, the purpose for which such information will be used, and the individuals or groups of individuals who will be authorized to access such information, and how the Sensitive Identifying Information will be used for data analysis. The agreement should also explain how the data will be returned or destroyed (see example 3 above).

Sample language: Notwithstanding any contrary terms, for Contractor's own use, Contractor shall be authorized to collect and analyze data and other information relating to the provision, use, and performance of various aspects of the [Services, defined term] and related systems and technologies in accordance with its privacy policy, except for Sensitive Identifying Information. Contractor may, however, during and after the term of this agreement, use Sensitive Identifying Information and other data in a de-identified, anonymized, pseudonymized, or aggregated form to improve and enhance the Services and for other development, diagnostic, and corrective purposes in connection with the Services and other Contractor offerings.

5. Restricting or Prohibiting Use of De-identified, Anonymized, Pseudonymized, or Aggregated Sensitive Identifying Information by Contractors

Question: Does the agency want to restrict or prohibit a contractor from using Sensitive Identifying Information in a de-identified, anonymized, pseudonymized, or aggregated form to conduct its own data analysis?

Guidance: If the agency wants to restrict or prohibit a contractor from using de-identified, anonymized, pseudonymized, or aggregated data that includes Sensitive Identifying Information other than for uses authorized in the agreement, the agreement should clearly and explicitly state such restrictions.

Sample language: Contractor shall not use or retain Sensitive Identifying Information for any use other than uses authorized in this Agreement, without Agency's prior written approval. This restriction applies to Sensitive Identifying Information in any form, including information that has been de-identified, anonymized, pseudonymized, or aggregated.

6. Public Statements or Press Releases Concerning Sensitive Identifying Information

Question: Does the agency anticipate that the contractor or its subcontractors will make any press or public statements regarding the services they provide or the information they access?

Guidance: If so, the agreement should include a statement explaining that the contractor or its subcontractors must notify the Agency about any press statement or publication related to the services or information.

Sample Language: If Contractor plans to issue any public statement, press release, or other publication in any media format regarding the services or information shared under this Agreement, it must send Agency written notice at least one week before issuing the anticipated statement.

The Contractor, and its officers, employees, and agents shall notify the Agency, at any time either during or after completion or termination of this Agreement, of any intended statement to the press or any intended issuing of any material for publication in any medium of communication (print, news, television, radio, Internet, etc.) regarding the services provided or the data collected pursuant to this Agreement at least 72 hours prior to any statement to the press, or at least five business days prior to the submission of the material for publication, or such shorter periods as are reasonable under the circumstances. The Contractor may not issue any statement or submit any material for publication that includes Sensitive Identifying Information or information otherwise designated as confidential under this Agreement.

7. Prohibition on the Sale or Monetization of Sensitive Identifying Information

Question: Will the contractor or its subcontractors seek to sell or monetize Sensitive Identifying Information, whether by direct request or as part of its general business model, policies and practices?

Guidance: Agencies' agreements with contractors, pursuant to which the contractor has access to Sensitive Identifying Information provided by the City or otherwise made available to the contractor in connection with the agreement, must include language prohibiting the contractor from selling or otherwise using or disclosing the

Sensitive Identifying Information for the contractor's financial benefit or other business need unless expressly authorized under the agreement.

Sample language: Except as otherwise provided in this Agreement, Contractor shall only use Sensitive Identifying Information for the purposes set forth in this Agreement and shall not disclose such information to any third parties, except as required by law. In addition, Contractor shall not use Sensitive Identifying Information for the benefit of another individual or entity, or publish, sell, monetize, license, distribute, or otherwise reveal such information.

Scope of Consent Guidance

Instructions

This guidance provides guidance implementing Citywide Privacy Protection Policies and Protocols Section 4.3.2 concerning consent. It also includes sample opt-in and opt-out consent forms for agency use.

These samples are for reference only; agencies should adapt them or create their own consent mechanisms. For example, verbal consent may be more appropriate for certain situations, and signatures may not be necessary.

Guidance on Consent Types and Scope

Opt-In Consent

Opt-in consent means obtaining an individual's consent ***before*** collecting, using, or disclosing that individual's identifying information. Opt-in consent may sometimes be required by law. Opt-in consent may also be appropriate based on evaluating the contextual integrity[4] of the identifying information. Opt-in consent may be appropriate when the collection, use, or disclosure involves sensitive identifying information, children's identifying information, disclosures to non-City entities, or uses of identifying information beyond the original purpose of the collection.

Opt-Out Consent

Opt-out consent means assuming consent by default but allowing an individual to affirmatively withhold consent to the collection, use, or disclosure of that individual's identifying information. Opt-out consent may sometimes be required by law. Opt-out consent may also be appropriate based on evaluating the contextual integrity of the identifying information. Opt-out consent may be appropriate when opt-in consent is impracticable and only non-sensitive identifying information is to be collected, used, or disclosed.

No Consent

Sometimes it may be inappropriate for an agency to allow for either opt-in or opt-out consent, such as if the collection, use, or disclosure of identifying information is required by law; if the identifying information is necessary to provide a benefit or service expressly requested by the individual; or identifying information is needed to assist in resolving exigent circumstances. Agencies should also evaluate the contextual integrity of the identifying information to determine other instances where not allowing for consent is appropriate.

[4] See CPO Policies and Protocols Sections 3.2.8 and 4.3.

Sample Consent Forms

Opt-In Consent Form

[Agency] will [collect/use/disclose] your identifying information[5] for [describe the purpose or use case "Purpose"].

(*If necessary*) [Law/regulation] requires [Agency] to obtain your consent before [collecting/using/disclose] your identifying information.

[Agency] will [collect/use/disclose your identifying information as follows:

Type of Identifying Information	Purpose of [Collection/Use/Disclosure]	Name of Entity [collecting/using/disclosing] identifying information

[Agency] will retain your identifying information for _____ [and/or] according to applicable citywide law and policy.

If you permit [Agency] to [collect/use/disclose] your identifying information for [Purpose], you may withdraw your consent at any time by contacting [Agency email]. If you withdraw your consent, [Agency] [will/will not] continue to use information that it obtained while your consent was in effect.

If you do not permit [Agency] to [collect/use/disclose] your identifying information for [Purpose], there will be [no consequences / the following consequences].

I hereby ___ permit / ___do not permit [Agency] to [collect/use/disclose] my identifying information for [Purpose].

_____

Name of Individual

_____

Name of Legal Representative (if applicable)

_____ _____

Signature of Individual or Legal Representative Date

[5] Defined at Admin. Code § 23-1201 as "any information obtained by or on behalf of the city that may be used on its own or with other information to identify or locate an individual."

Opt-Out Consent Form

[Agency] is [collecting/using/disclosing] your identifying information[6] for [describe the purpose or use case "Purpose"].

(*If necessary*): [Law/regulation] requires [Agency] to obtain your consent before [Agency] may continue [collecting/using/disclosing] your identifying information.

[Agency] is [collecting/using/disclosing] your identifying information as follows:

Type of Identifying Information	Purpose of Collection/Use/Disclosure	Name of Entity collecting/using/disclosing identifying information

[Agency] will retain your identifying information for _____ [and/or] according to applicable citywide law and policy.

If you do not permit [Agency] to [collect/use/disclose] your identifying information for [Purpose], there will be [no consequences / the following consequences].

I hereby request [Agency] to stop [collecting/using/disclosing] my identifying information for [Purpose].

_____
Name of Individual

_____
Name of Legal Representative (if applicable)

_____ _____
Signature of Individual or Legal Representative Date

[6] Defined at Admin. Code § 23-1201 as "any information obtained by or on behalf of the city that may be used on its own or with other information to identify or locate an individual."

Guidance for Assessing Online Analytics

Online analytics can track and collect identifying information without user knowledge or consent, and then analyze and infer information about their behavior, assess campaign effectiveness, and establish an audience for targeted advertising. Based on users' online interactions as well as data from external sources, third-party analytics providers can gain comprehensive insights about users, and they can provide useful performance metrics to website operators.

Assess Privacy Considerations. City agencies and contractors should assess privacy considerations before deploying online analytics on their websites or apps. Agencies should consider their business purposes for using online analytics and weigh the underlying privacy risks associated with accomplishing these purposes. The Privacy Impact Assessment template can serve as a reference point for agencies to think through the issues and risks involved. If possible, consider whether agency-operated analytics are suitable for the business purpose.

Agencies should be able to articulate, for each online analytics tool, the business purpose for the use of online analytics; the agency program supported by the use of online analytics; the placement of and business purpose of each type of identifying information collected and disclosed by the online analytics; and an explanation for why alternatives are insufficient for the agency's business purpose.

Inform Users. Additionally, City agencies should, whenever feasible, inform users about the potential collection or disclosure of their identifying information to third parties in a manner that is clear to users of varying levels of expertise, and clearly explain why the information is being shared. Agencies should actively work to reduce the risks posed by online analytics by offering users an opt-out option, requiring third-party analytics providers to refrain from selling or sharing collected identifying information, and limiting how long identifying information is retained.

Review Third-Party Analytics. Agency privacy officers should pay special attention to online analytics that send information to a third party and return generalized statistics to the agency. In such cases, the third party often receives identifying information about the user and can combine it with information that it already has.

Consult with Other Stakeholders. Agency privacy officers should periodically collaborate with other stakeholders at their agency, which may include their agency chief information security officer, agency website development staff, and the Office of Technology and Innovation, to assess the privacy and cybersecurity impact of digital analytics tools that are actively in use or under consideration.

Identifying Information Law Primer

Introduction and Personnel

The **Identifying Information Law** (IIL) is **New York City's privacy law**.[7] The IIL enables City agencies[8] to protect the privacy of City residents' identifying information while providing benefits and services to the public by requiring each covered agency to appoint an agency privacy officer (APO). The IIL also created the role of the **Chief Privacy Officer** (CPO), the City's authority on privacy-related matters. The Chief Privacy Officer is the head of the **Office of Information Privacy** (OIP), and both are located in the **Office of Technology and Innovation** (OTI).

The Chief Privacy Officer also promulgates citywide privacy policy based on the IIL, chiefly the **Citywide Privacy Protection Policies and Protocols** (CPO Policies). Agency privacy officers are responsible for administering and implementing the IIL and the Chief Privacy Officer Policies, including approving agency collections and disclosures of identifying information and reporting on their agencies' collections and disclosures. Agency privacy officers also serve as point persons for their agencies' overall privacy matters.

What is Identifying Information?

The Identifying Information Law governs the collection and disclosure of identifying information by City agencies and their covered contractors and subcontractors. **Identifying information** is any information that may be used on its own or with other information to identify or locate an individual. This can include even mundane details such as clothing type under the proper circumstances. **Sensitive identifying information** is identifying information that can pose a greater risk of harm if improperly disclosed to unauthorized individuals.[9] This can include information such as Social Security numbers and domestic violence status. It requires additional safeguards to protect its privacy and security.[10]

[7] Admin. Code §§ 23-1201 to 1205.
[8] Agencies include borough presidents' offices and community boards, but do not include certain City-related entities such as district attorneys, the Department of Education, and Health + Hospitals Corporation.
[9] E.g., harm related to finances, health, or protected status.
[10] E.g., it must be classified as "Restricted" under the Citywide Cybersecurity Program Policies and Standards and can only be disclosed through a written data-sharing agreement.

How Agency Privacy Officers Work

City agencies may not collect or disclose identifying information without approval from their agency privacy officers. Agency privacy officers can approve collections or disclosures of identifying information to or from their agencies if:

- Required by law[11] or treaty;
- It furthers their agency's mission or purpose;[12]
- With the consent of the person to whom the information pertains.

Agency privacy officers must approve collections and disclosures in writing. They must also designate approvals as either **routine** or **case-by-case**. Agency privacy officers can change designations at their discretion.

- For **case-by-case** approvals, an agency privacy officer approves each separate collection or disclosure of identifying information for a particular agency function. Case-by-case approvals can be made for unique or one-time agency projects or circumstances. Agency privacy officers record case-by-case approvals on **Form 5.**
- **Routine** approvals are for collections and disclosures of identifying information that occur frequently or during the normal course of agency business. An agency privacy officer makes a routine approval by approving all occurrences of one type of collection or disclosure at once. Routine approvals can be made for common agency functions, such as human resources administration (e.g., hiring) or replying to legal requests (e.g., Freedom of Information Law requests or subpoenas). Agency privacy officers record routine approvals on **Form 2**.
- **Exceptions** (collections or disclosures that do not require agency privacy officer approval):
    - Collections or disclosures under exigent circumstances;[13]
    - Collections or disclosures concerning an open New York City Police Department investigation of a committed, impending, or attempted crime;
    - Collections or disclosures concerning an open welfare investigation of a minor or legally incompetent person.

If an APO determines that the collection or disclosure does not further their own agency's mission or purpose (e.g., disclosing identifying information for the federal census), the APO can request the CPO approve the collection or disclosure in the best interest of the City. The CPO can only approve best interests of the City disclosures to City agencies.

[11] Including court orders.
[12] APOs should consult various sources to determine agency mission or purpose, including their agency's enabling statute, former and current projects, and mission statements from agency documents or their agency's website.
[13] Situations where the collection or disclosure is so urgent that obtaining APO approval may cause undue delay (i.e., emergencies such as a building fire or gas explosion).

Identifying Information Law Compliance Reporting

Quarterly: Exigent Circumstances and Disclosures in Violation of the Identifying Information Law

Agency privacy officers must record (1) agency disclosures of identifying information in violation of the Identifying Information Law and (2) collections or disclosures of identifying information under exigent circumstances on the **Identifying Information Law Notification Form**.[14] Agency privacy officers may submit these forms to the Office of Information Privacy at any time, but must submit any pending forms by the end of each quarter.[15] Office of Information Privacy summarizes and anonymizes them to create publicly available reports submitted by the Chief Privacy Officer to the Speaker of the City Council.[16]

Agency privacy officers should nevertheless notify Office of Information Privacy of these matters at oip@oti.nyc.gov within 24 hours of discovery so Office of Information Privacy can work with City partners, such as Cyber Command and the Law Department, to address them immediately.

Agencies must also notify individuals affected by a violation in disclosure of the Identifying Information Law if:

- Required by law or treaty;
- There is a potential risk of harm to an individual to whom the information pertains;[17] or
- The agency so determines after consultation with the Chief Privacy Officer and other City partners.

Biennial: Agency Privacy Reports

Every two years, agency privacy officers must provide an overview of their agency policies and practices relating to identifying information on the **Biennial Agency Report**. To complete a Biennial Agency Report, agency privacy officers should consult the agency's internal inventory of collections and disclosures of identifying information on **Worksheet 1** and **Worksheet 2** , which they should update regularly based on Forms 2 and 5.

Agency privacy officers must submit Biennial Agency Reports to the Chief Privacy Officer, the Mayor, the Speaker of the City Council, and the **Citywide Privacy Protection Committee**, a select group of representatives designated by the Identifying Information Law and the Mayor. The Citywide Privacy Protection Committee reviews all submitted Biennial Agency Reports and issues recommendations on how the Chief Privacy Officer should update citywide privacy policy. The Chief Privacy Officer can implement the recommendations by revising the Chief Privacy Officer Policies or by issuing additional guidance. The Office of Information Privacy also regularly convenes the Citywide Privacy Protection Committee to discuss any privacy issues affecting the City.

---

[14] A disclosure in violation of the IIL means any circumstance where the APO did not approve the disclosure, e.g., intentionally or inadvertently sending identifying information to the wrong recipient, theft or improper disposal of identifying information, or access to identifying information as a result of a potential security incident.
[15] The quarters end on March 31, June 30, September 30, and December 31.
[16] See "Chief Privacy Officer's Agency Disclosures" in the link.
[17] E.g., harm related to finances, health, or protected status.

Other Aspects of the Identifying Information Law

The Identifying Information Law's Interaction with Other Laws

If a state or federal law requires the collection or disclosure of identifying information, the agency should follow the law, and the agency privacy officer must provide written approval of the collection or disclosure in accordance with the IIL. If a state or federal law does not require a collection or disclosure but permits it, the Identifying Information Law is still applicable: the agency privacy officer can only approve the collection or disclosure if it furthers their agency's mission or purpose.

Contracts

The Identifying Information Law also applies to covered contractors and subcontractors. The contracts currently covered are:

- Contracts for **human services**[18]
- Contracts for **technology services** involving **sensitive identifying information**[19]
- Contracts to provide **outreach services** for an agency other than the agency contracting for the outreach services[20]

The Chief Privacy Officer may designate additional types of covered contracts. The **Identifying Information Rider** must be attached to covered contracts. Office of Information Privacy recommends attaching the **Privacy Protection Rider** to non-covered contracts, otherwise appropriate privacy protection terms should be included.

Oversight Agencies

- Agency privacy officers can approve requests for identifying information from oversight agencies as routine or case-by-case.[21]
- If a request for identifying information from an oversight agency risks compromising an important privacy interest (such as the disclosure of sensitive identifying information):
    - If both agencies are covered by the Identifying Information Law, a data-sharing agreement and secure transmission and storage protocols are required for disclosure to the oversight agency.
    - If one or both agencies are not covered by the Identifying Information Law, a data-sharing agreement is recommended for disclosure to the oversight agency.

[18] Services provided to third parties (e.g., social, health, legal, employment assistance, or educational services).
[19] Effective for new contracts or those renewed on or after July 1, 2021. See CPO Policies 6.1.2.1 for examples.
[20] See CPO Policies 6.1.2.2. An example would be a citywide initiative conducted by a lead agency to provide services to City residents where a contractor would collect identifying information of another agency's clients to contact them about available services or notify them about an upcoming information session.
[21] The oversight agency must be legally entitled to request the identifying information, and the agency receiving the request cannot be legally restricted from disclosure nor be asserting a privilege to the information.

Privacy Flyer for Employees

Do Your Part to Protect Identifying Information!

The City's Identifying Information Law protects identifying information. Identifying information is any information that can identify or locate a person. This includes names, addresses, and phone numbers, but also things like being eligible to receive City benefits or services.

As an employee of the City, you can't collect or disclose identifying information outside your agency without permission from your agency privacy officer. But that's OK! Your agency privacy officer has already approved certain collections and disclosures. So get to know your agency privacy officer and how to contact them if you have any questions.

If you find out identifying information has been mishandled in any way (like being sent to the wrong person), you should report it to your agency privacy officer immediately. Protecting identifying information is important for City residents' privacy and security.

Thank you for doing your part to protect identifying information!

REMEMBER: Think before you share! When in doubt, don't give it out!

Sample Training Slides

Identifying Information

is "any information obtained by or on behalf of the city that may be used on its own or with other information to identify or locate an individual"

- **Obtained by or on behalf of the City** – includes all contractors or volunteers or employees and the like.
- **Identify or locate an individual** – some types of information easily fall into the definition, like name and social security number.
- **On its own or with other information** – if the information can be linked with other information to identify or locate an individual, then the information is identifying.

NYC OTI Information Privacy

Role of the Agency Privacy Officer

- The agency privacy officer ***approves collections and disclosures*** of identifying information.
- The agency privacy officer also has a ***duty to report*** to the Chief Privacy Officer ***within 24 hours*** of becoming aware of certain collections and disclosures.

Talk to your agency privacy officer as soon as possible when

- You ***suspect*** a ***disclosure*** was ***not approved***.
- You or any employee collects or discloses identifying information in an ***emergency***.

NYC OTI Information Privacy

Contact the Agency Privacy Officer

Contact {insert APO name} at {insert email address}.

"When in doubt, don't give it out!"

NYC OTI Information Privacy

Template Agency Privacy Officer Introductory Email

Subject: Welcome from your new agency privacy officer

[Agency] colleagues,

I'd like to introduce myself as [agency]'s agency privacy officer. My role is to help you understand how to handle identifying information in your work, and help [agency] comply with its privacy obligations.

As you know, [agency] handles an enormous amount of information for the City, some of which the City's Identifying Information Law classifies as *identifying information* (information that can be used to identify or locate a person). We are all responsible for properly handling identifying information.

The Identifying Information Law requires City employees to follow certain processes when collecting, using, disclosing, or accessing identifying information. You can learn more about this by reviewing materials from the City's Office of Information Privacy, an office within the City's Office of Technology and Innovation that handles Citywide privacy questions and is headed by the City's Chief Privacy Officer, Michael Fitzpatrick.

If you have questions about how you use identifying information in your work at [agency], please contact me. You may also hear from me as I learn more about the information [agency] handles, so thank you in advance for your assistance in helping me understand your work. The Office of Information Privacy is available as an additional resource if you have privacy questions.

Template Agency Privacy Officer Annual Email

Subject: Reminder from your agency privacy officer

[Agency] colleagues,

I hope you had a wonderful [year]. As [agency's] agency privacy officer, my role is to help you understand how to handle identifying information in your work, and help [agency] comply with its privacy obligations. [Agency] may need to report some information on a quarterly basis, and must do so on a biennial basis. I may reach out for information or assistance with these reports.

As you know, [agency] handles an enormous amount of information for the City, some of which the City's Identifying Information Law classifies as identifying information (information that can be used to identify a person). We are all responsible for properly handling identifying information.

The Identifying Information Law requires City employees to follow certain processes when collecting, using, disclosing, or accessing identifying information. You can learn more about this by reviewing materials from the City's Office of Information Privacy, an office within the City's Office of Technology and Innovation that handles Citywide privacy questions and is headed by the City's Chief Privacy Officer, Michael Fitzpatrick.

If you have questions about how you use identifying information in your work at [agency], please contact me. The Office of Information Privacy is available as an additional resource if you have privacy questions.

Model Guidance to Agency Staff

Background

New York City's Identifying Information Law governs how City agencies and their contractors collect, use, disclose, access, and retain identifying information. The City has a Chief Privacy Officer, who issued the Citywide Privacy Protection Policies and Protocols to implement the Identifying Information Law.

Your agency head and agency privacy officer are responsible for ensuring that your agency complies with the Identifying Information Law and Citywide Privacy Protection Policies and Protocols. If you have access to identifying information, then *you* are responsible for protecting it.

What is identifying information?

Identifying information is any information obtained by or on behalf of the City that may be used on its own, or with other information, to identify or locate an individual. Identifying information not only includes information about clients and residents served by the agency, but also includes information about City agency employees and officials. Some common types of identifying information are listed in the Citywide Privacy Protection Policies and Protocols. Keep in mind that information can be identifying even if it's not on the list.

Some types of identifying information pose a higher risk of harm to an individual or members of an individual's household if not properly protected. These types of information are "sensitive identifying information" and need greater protection.

Your responsibilities as a City employee or contractor

Limit access and use for job purposes: Only access identifying information if you have a legitimate business need related to performing your duties. If you have access to identifying information when you should not, immediately notify your agency privacy officer.

Ask for agency privacy officer approvals: You are not allowed to collect or disclose identifying information without permission from your agency privacy officer. Your agency privacy officer has approved certain collections and disclosures of identifying information as "routine" for your agency. You **do not** need to ask your agency privacy officer for permission to collect or disclose identifying information when the agency privacy officer has approved it as routine. If you want to collect or disclose identifying information for a purpose that the agency privacy officer has not approved as routine, you must first consult with your agency privacy officer. And if the privacy officer has already approved collection or disclosure of identifying information for an agency purpose, but you want to collect or disclose a new type of identifying information for that purpose, you must first contact the privacy officer for approval.

Sometimes your agency privacy officer will approve a collection or disclosure on a case-by-case basis, such as for a limited time or for a specific circumstance. In those cases, you must ask your agency privacy officer for permission to collect or disclose identifying information outside of those times or circumstances.

If you are not sure whether a collection or disclosure has been approved, ask your supervisor or the agency privacy officer.

There are some circumstances in which you may collect or disclose identifying information without permission from the agency privacy officer, such as to the police department in connection with an investigation of a crime, in connection with an open investigation by a city agency concerning the welfare of a minor or an individual who is otherwise not legally competent, or under exigent circumstances. Consult with your agency privacy officer to learn more.

Report unauthorized collections or disclosures: Contact your agency privacy officer as soon as practicable if you suspect you, another employee or contractor, or a third party has collected or disclosed identifying information without authorization (whether intentionally or not). Your agency privacy officer is responsible for investigating any potential violation of the Identifying Information Law.

The agency privacy officer's primary focus is to ensure that the agency's policies and procedures are followed to protect the privacy of individuals and to prevent unauthorized collections or disclosures from occurring in the future. While the agency takes all violations of the Identifying Information Law seriously, the privacy officer's role is to identify and address any issues and ensure compliance, rather than to punish individuals for past mistakes.

Chief Information Security Officer Template Agenda

Agency Meeting: Privacy and Security

Agenda

- *Introductions*
  - *Get to know each other and your teams/work*
  - *Role of the agency privacy officer*
- *Projects Sync*
  - *What are projects on each of your desks? Can you collaborate?*
  - *Are there upcoming data sharing needs to discuss?*
- *Particular Concerns*
  - *Privacy matters or goals*
  - *Security incidents or goals*
- *Breach Protocol and Best Practices*
  - *Are you aligned on communication, notification, and mitigation protocol?*
  - *Are there practices you might want to effectuate at the agency?*
  - *Is there any education or communication to staff that would promote your work or goals?*
- *Artificial Intelligence*
  - *Have any requests been made to use artificial intelligence tools? What is the status of the requests?*
  - *Have these requests been approved by the Agency CISO?*
  - *Do requests to use artificial intelligence tool involve the use of sensitive identifying information or Restricted City Data?*
  - *How can we become aware of unapproved uses of artificial intelligence tools at the agency? How can we encourage compliance?*
  - *What is the status of the agency's SharePoint or other document-sharing permissions-management efforts?*

Agency Head Template Agenda

Agency Meeting: Privacy policy and Business updates

Agenda

- *Introductions*
  - *Re-introduce role of the agency privacy officer*
  - *Describe day to day and/or tasks*
  - *Review agency privacy officer checklist*
  - *Discuss agency objectives for privacy and how agency privacy officer can help effectuate*
- *Review of Collections and Disclosures*
  - *Go over current collections, disclosures and practices*
  - *Review existing Identifying Information Law forms and update*
  - *Are there new needs or collections anticipated in initiatives? Are there requests for disclosure?*
- *Particular Concerns or Challenges*
  - *Privacy matters or goals*
  - *Security incidents or goals*
  - *Are there resources, educational efforts, or projects that would benefit your agency's privacy practice?*
- *Projects on the Horizon*
  - *What are the agency's priority projects? Is there a privacy impact?*
  - *Are there upcoming data sharing needs to discuss?*

Business Head Template Agenda

Agenda

- *Introductions*
  - *Get to know each other*
  - *Re-introduce role of the agency privacy officer*
  - *Describe day to day and/or tasks*
  - *Discuss business head objectives and how the agency privacy officer work may be involved*
- *Review of Collections and Disclosures*
  - *Review existing Identifying Information Law forms and update related to Business Head operations*
  - *Are there new needs or collections anticipated in initiatives? Are there requests for disclosure?*
- *Particular Concerns or Challenges*
  - *Privacy matters or goals*
  - *Security incidents or goals*
  - *Are there resources, educational efforts, or projects that would benefit business head's work or team?*
- *Projects on the Horizon*
  - *What are the agency's priority projects? Is there a privacy impact?*
  - *Are there upcoming data sharing needs to discuss?*

Sample Agency Identifying Information Complaint Form

Report Related to the Identifying Information Law

If you believe that [agency] or one of its contractors has collected, retained, or disclosed identifying information in violation of the Identifying Information Law (Admin. Code §§ 23-1201 through 23-1205), you may fill out and submit this form.

Name:

Your Name

Email:

Your Email

Phone:

Your Phone Number

Date you learned that [agency] collected or disclosed identifying information:

mm/dd/yyyy

Description:

Provide a detailed description of the issue...

Submit Complaint

Complaints will be sent to the [agency]'s privacy officer and will only be used to investigate this complaint. To investigate and resolve the complaints, [agency] may share complaint information with other City agencies.

Model Investigation Plan

Instructions

This section provides a model plan and guidance on how to respond to incidents when the security of identifying information may have been compromised. In responding to incidents, agencies should start with (1) the Citywide Incident Response Policy and (2) the Agency Incident Response Readiness Program. This section is geared primarily toward the investigation of cybersecurity incidents because of their prevalence, but not all incidents requiring investigation are related to cybersecurity issues (e.g., misdirection of correspondence to an unintended recipient). The agency privacy officer must coordinate with the agency chief information security officer when a cybersecurity incident is implicated. The guidance below is applicable to privacy-related incidents as well and is intended to supplement Cyber Command's published directives. Agencies should revise this model investigation plan to suit their specific circumstances.

Keep in mind that an incident may implicate other City entities as well, such as when multiple agencies use the same contractor. Depending on the circumstances, it may be appropriate to manage the investigations jointly. Further guidance on handling such circumstances is provided below.

The guidance includes a sample notification letter and credit monitoring supplement, instructions for accessing the citywide breach notification and credit monitoring contract, and starter questions for different kinds of incidents. Please visit the Office of Information Privacy's intranet page for supplemental and updated materials and annotated and editable versions of these documents.

All capitalized terms are as defined in the Citywide Cybersecurity Program Glossary.

Establish an incident response team and coordinated communication channels: An incident response team is a group of individuals who are responsible for coordinating and managing the response to an incident. The incident response team should be composed of individuals with the necessary skills and expertise to handle a variety of potential incidents. The incident response team may respond to both privacy and cybersecurity incidents. Ensure that the incident response team members can communicate effectively during an incident. This may include having and testing separate phone numbers, email addresses, or even out-of-band communications if an agency's network is down. The members of the incident response team should also be familiar with each other and comfortable with raising issues to the other members.

Identify and document potential risks and vulnerabilities: Conduct a risk assessment to identify potential threats and vulnerabilities that could result in an incident.[22] Engage with agency stakeholders, cybersecurity professionals, agency counsel, and business heads to understand the unique risks the agency faces because of its posture, technical and legal environment, or other factors. Consider different types of incidents:

- Loss, theft, or improper disposal of devices such as (1) agency-issued cell phones, CDs, thumb drives, portable devices, desktop computers, laptops, photocopiers, fax machines; or (2) employee-owned devices used for agency purposes (**Bring Your Own Device** or **BYOD**).
- Loss, theft, or improper disposal of hard copy documents that contain Information (including Identifying Information), regardless of whether such Information is Restricted, Sensitive, Non-Restricted, or Public Data per the Citywide Data Classification Standard or Citywide Information Management Standard.
- Release of Information in response to a fraudulent email or telephone call (**phishing**).
- Unauthorized disclosure of Information to the internet or any social media sites.
- Unauthorized copying of Information to personal Devices such as routers, thumb drives, etc.
- Penetration, compromise, unauthorized access, or malware infection of a vendor's network.

Receive reports: The agency may learn of incidents in many ways, such as employee reports, notifications from Cyber Command or the Office of Information Privacy, or complaints from the public. The agency should establish and publicize mechanisms for people to report suspected incidents to the agency.

Activate the incident response team: When a report is received through any mechanism, the person receiving the report should immediately notify the relevant members of the incident response team. The incident response team members will coordinate to include resources to respond to the incident. All incident investigations are confidential. Contact information for the incident response team should be contained in the agency's incident response plan. Not all complaints or incidents that impact privacy are cybersecurity matters. For suspected

[22] Agencies may find it helpful to consult the questions in the Privacy Impact Assessment on the administrative, physical, and technical controls used to restrict unauthorized access to identifying information.

cybersecurity incidents, agencies and agency privacy officers coordinate with their cybersecurity staff and should contact Cyber Command at by email at [redacted] or [redacted], or by phone at 718-403-6761. Cyber Command monitors these lines of communication at all hours.

Except as directed by Cyber Command, Office of Information Privacy, or the Law Department or agency counsel, the agency privacy officer should limit communication regarding any investigation to these offices and to personnel directly engaged in the investigation and should use the agency's preferred method of communication. All information relating to an incident should be designated as "Restricted" under the Citywide Cybersecurity Program Policies and Standards.

Because the Office of Information Privacy supports agencies citywide, it may be aware of similar incidents affecting other agencies. If, based on the circumstances of an incident, the Office of Information Privacy determines that the incident affects multiple agencies, it will communicate individually with the agency privacy officer of each affected agency to obtain consent to a joint investigation. For cybersecurity incidents, it may coordinate with Cyber Command on whether a joint investigation of the incident is advisable. No information relating to an agency's incident investigation will be shared with another agency by the Office of Information Privacy unless the agency has consented to a joint investigation.

There may be instances when an agency has experienced an unauthorized disclosure or collection of identifying information due to actual or suspected criminal activity. It may be appropriate for the agency to contact the New York City Police Department to make a report. By informing the New York City Police Department about an incident, an agency can get assistance with mitigating risks, recovering property, and potentially pursuing criminal charges.

Agency privacy officers should be guided by agency counsel in determining when to report an incident to the New York City Police Department. When reporting an incident to the New York City Police Department, the agency should contact the New York City Police Department's agency privacy officer at [redacted], who will gather information and direct the agency on specific next steps, such as how and where to file a police report.

Investigate: The agency privacy officer is responsible for maintaining a confidential record of the investigation that, at the outset, should include the name and contact information of the party reporting the incident, the date and time the incident was reported, and the date and time the incident is believed to have occurred (if known). The agency privacy officer will add to the investigation record as they proceed with the fact-gathering process.

Not every incident is a Cybersecurity Event of Interest (**EoI**) or a Cybersecurity Incident. The initial fact-gathering will help determine the nature of the incident and the parties to be engaged in the subsequent investigation. Depending on the circumstances of the incident, it may be possible to mitigate the effects of a suspected compromise. For example, if the incident involves the loss of physical Devices, the agency privacy officer should make sure the incident response team has thought through all the locations for where the Devices might be. If an

email or fax was sent to the wrong recipient, it may be possible to retract the correspondence or ask the recipient to delete it.

If the incident is a Cybersecurity Event of Interest or Cybersecurity Incident, the agency chief information security officer is the technical lead for the cybersecurity or technical investigation. Again, the first goal should be to contain and mitigate the effects of the EoI or incident. The agency chief information security officer, working with the agency privacy officer and Cyber Command, should make the determination on whether and how to take compromised Assets off-line or otherwise isolate them to contain the issue in a manner that allows for the collection and preservation of any relevant evidence while also enabling the continuation of normal Agency functions.

Each incident is unique, so asking pertinent questions is an important step toward ultimate resolution. The fact-gathering process may extend beyond the initial phase of the investigation, as answers to these questions may generate leads for follow-up. The agency privacy officer should work closely with their agency counsel, agency chief information security officer, and Cyber Command to obtain information requested by the forensics team.

Attached to this procedure are sample questions for different types of incidents that may be helpful to agency privacy officers as a starting point to their investigations. Agencies should add questions specific to the circumstances of each incident to the sample questions. If an agency contractor is involved, consider whether to request information using the reporting provisions of the Identifying Information Rider, Privacy Protection Rider, or other contract terms.

Communicate: The incident response team should communicate with relevant parties, including agency management, the Office of Information Privacy, Law Department, and Cyber Command, to keep them informed about the status of the investigation and any actions that are being taken. All written communications relating to an investigation should be designated as “Restricted.”

For incidents involving identifying information, the agency privacy officer must notify the Office of Information Privacy within 24 hours after learning of the incident, even if not all the details are fully known. The Office of Information Privacy will help ensure that other components of the Office of Technology and Innovation, such as Cyber Command, are aware of the incident.

Avoid speculation: Throughout the investigation but particularly during the early stages, the agency privacy officer should encourage all personnel involved in the investigation to avoid speculating about the facts and to avoid using conclusory terms like “breach,” “fault,” “negligence,” etc. in all communications.

Conduct a legal assessment: The agency privacy officer, in collaboration with the agency’s counsel, Law Department, Chief Privacy Officer, and others, will review the facts pertaining to the incident and assess whether a violation of the Identifying Information Law or other laws has occurred. They will identify the agency’s legal obligations, including whether to notify individuals affected by the incident. Please note that in joint investigations, each affected agency remains responsible for conducting the legal assessment for their agency.

Decisions regarding whether, when, and how to notify individuals may be contingent on different legal frameworks applicable to the affected agencies, or on other agency-specific considerations.

NYC Admin. Code 10-502 requires that when an agency discovers a breach of security, and private information was, or is reasonably believed to have been accessed, acquired, disclosed, or used by an unauthorized person, notice must be given to any individual whose Identifying Information is reasonably believed to have been disclosed to or accessed by an unauthorized party. If 5,000 or more New York residents are affected, notification must be made to consumer reporting agencies as well. There may be additional requirements applicable to specific types of Information or agencies, such as when protected health information or student information is involved. Refer to the notification chart for a summary of some of the common notification frameworks.

If the incident response team determines that the Identifying Information Law or other laws have been violated, it must develop a plan of action that will meet the agency's legal obligations, including whether notification to affected individuals is legally required or is prudent. The agency privacy officer must also file a report with the Chief Privacy Officer documenting the violation.

If the incident involves a product or service provided or managed by a third party, the agency privacy officer and agency counsel will need to review the relevant contract documentation to determine whether the vendor has performed its contractual obligations. Recommended starting places are the contract's limitation of liability, representations and warranties, indemnities, and confidentiality provisions.

Issue notifications: If it has been determined that notification to individuals must or should occur, the agency must determine the universe of individuals to be notified, the method of notification, whether any regulators need to be advised before notifications are issued, draft the notification content, and secure credit monitoring services, if necessary, through the citywide credit monitoring contract.

Document and close-out: At the end of the incident, the agency privacy officer should work with the agency general counsel to (1) document the circumstances of the incident and the actions taken by the engaged parties and (2) describe in non-technical terms any remediation measures taken. If the incident was determined to be a Cybersecurity Event of Interest or Cybersecurity Incident that was investigated by Cyber Command, Cyber Command will complete an Incident Report that summarizes its root-cause findings.

Suggested Initial Investigation Questions.

Questions about Potentially Affected Data

The following are some typical questions to consider at the outset of an investigation regarding the nature of the potentially compromised data. This is intended only as a starting point and is by no means an exhaustive list; as the investigation unfolds, additional questions are likely to arise.

- What is the nature of the Information that was potentially compromised?
- Does the Information include Restricted Information?
- Does the Information include Sensitive Information?
- Does the Information contain Identifying Information?
- Does the Information include information that is governed by other regulatory frameworks (e.g., Protected Health Information under HIPAA)?
- Does the incident involve information that personnel from other agencies are not authorized to access?
- If the Information is Identifying Information, how many individuals are potentially affected?
- Does the Information contain the personal information of non-NY residents? What kind – health, financial, or personal details?
- Do we have reason to believe the Information has been, or is likely to be exploited in some way?
- What harm could ensue if the Information is exploited?
- Will the affected individuals be notified of the potential compromise?

Questions for a Privacy-Related Incident

The following are some typical questions to consider at the outset of an investigation into a privacy-related incident such as the loss/theft of a physical Device, the loss/theft of hard copies of materials, or the misdirection of materials to unintended recipients. This is intended only as a starting point and is by no means an exhaustive list; as the investigation unfolds, additional questions are likely to arise.

- Basic facts of the incident -- what form of information was lost -- physical Device? Hard copies? Misdirected correspondence? When?
- If the incident involves misdirected correspondence, have the unintended recipients been asked to delete the email/dispose of the materials? [ATTEMPT TO MITIGATE]
- If the incident involves the loss/theft of a Device, can the Device be wiped remotely? [ATTEMPT TO MITIGATE]
- If the incident involves the loss/theft of a Device, is the Device protected with a strong password?
- If the incident involves the loss/theft of a Device, is multi-factor authentication required to access City/Agency systems?
- If the incident involves the loss/theft of a Device, is the Device encrypted?
- If the incident involves the loss/theft of a Device, what type of Device? How many endpoints/users are associated with the Device? (e.g., a City-issued cell phone would typically have only one user, while a laptop might have several users, depending on how it's used. The answer will help drive how many user accounts will need to be looked into for indicia of compromise.)
- If the incident involves the loss/theft of a Device, what type of work does the owner/user of the Device do?
- If the incident involves the loss/theft of a Device, what kind of Information does the owner/user have access to? Did the owner/user access this Information using the lost Device?
- If the incident involves the loss/theft of a Device, is there reason to believe the owner/user was targeted?
- If the incident involves the loss/theft of a Device, does the Device contain any Identifying Information of the owner/user?
- Does the Information that was lost contain Restricted Information or Identifying Information?
- Regardless of the form of the compromised Information, is there any indication that the Information has been or is likely to be accessed?
- When did the agency or contractor become aware of the incident?

- Which employees or contractors have information relating to the incident?
- Which types of identifying information are potentially impacted?
- If a third party is involved, do they have privacy counsel?
- Is there a forensic report? If there are multiple reports, do they differ?
- Have law enforcement or regulatory agencies need to be notified? Have they already been notified?

Summary of Notification Laws				
Law	**Information covered**	**Applicability**	**Trigger**	**Notification requirements**
NYC Disclosure of Security Breach Law New York City Admin. Code 10-501 *et seq.*	A) Username or e-mail address in combination with a password or security question and answer; or B) Any information re an individual that because of a name, number, symbol, mark or other identifier, can be used to identify that individual; plus any one or more of 1) SSN; 2) driver's lic. number or non-driver ID number; 3) acc't number, credit or debit card number, in combination with any security code, access code, password or other information that would permit access to an acc't; 4) acc't number, or credit or debit card number, if such number could access an acc't without additional information; or 5) biometric information	Agencies that own or license computerized data that includes private information	Unauthorized access, acquisition, disclosure or use of computerized data that compromises the security, confidentiality or integrity of private information maintained by an agency	Notice to affected individuals as soon as practicable If more than 5,000 New York residents are to be notified, then notice to consumer reporting agencies

Summary of Notification Laws				
Law	**Information covered**	**Applicability**	**Trigger**	**Notification requirements**
NY SHIELD Act General Business Law 899-AA (Not applicable to City agencies; applies to private entities experiencing a breach)	A) Username or e-mail address in combination with a password or security question and answer; or B) Any information re an individual that because of a name, number, symbol, mark or other identifier, can be used to identify that individual; plus any one or more of 1) SSN; 2) driver's lic. number or non-driver ID number; 3) acc't number, credit or debit card number, in combination with any security code, access code, password or other information that would permit access to an acc't; 4) acc't number, or credit or debit card number, if such number could access an acc't without additional information; 5) biometric information; 6) medical information; or 7) health insurance information	Person or business that owns or licenses computerized data that includes private information	Unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business	Notice to the owner of the affected data Notice to affected New York residents in the most expedient time possible and within 30 days after a breach is discovered Notice to attorney general, department of state, division of state police, and department of financial services If more than 5,000 New York residents are to be notified, then notice to consumer reporting agencies

Summary of Notification Laws				
Law	**Information covered**	**Applicability**	**Trigger**	**Notification requirements**
NYC Identifying Information Law New York City Admin. Code 23-1201 *et seq.*	Any information obtained by or on behalf of the city that may be used on its own or with other information to identify or locate an individual	Agencies Covered contractors	Required by law, when there is potential risk of harm to an individual, or when prudent	Notice to Chief Privacy Officer within 24 hours Notice to affected individuals as soon as practicable
NY Social Security Number Protection Law General Business Law 399-DDD	Social Security numbers	Persons, firms, partnerships, associations or corporations; not the City	Lack of reasonable procedures to protect Social Security numbers or intentional unauthorized access to Social Security numbers	Notice to attorney general
Health Insurance Portability and Accountability Act (HIPAA) 45 CFR Part 164.400-414	Protected health information -- individually identifiable health information held or transmitted by a covered entity or its business associate	Health plans, health care providers, healthcare clearinghouses, business associates. Applies to City agencies that are "covered entities" or "business associates."	Disclosure of PHI other than as permitted by the HIPAA Privacy Rule (45 CFR Part 160 and Part 164, Subparts A and E)	Written notification to affected individuals within 60 days; annual reporting to HHS unless 500 or more affected, in which case reporting is required within 60 days; notice to NYS Attorney General within 5 business days of notification to HHS; notice to "prominent media" within 60 days if 500 or more affected

Summary of Notification Laws				
Law	**Information covered**	**Applicability**	**Trigger**	**Notification requirements**
Federal Trade Commission Health Breach Notification Rule (HITECH) 16 CFR Part 318	Unsecured electronic health information that could reasonably be used to identify an individual	a vendor of personal health records (PHRs); a PHR related entity; or a third-party service provider for a vendor of PHRs or a PHR related entity	Unauthorized acquisition or disclosure of unsecured electronic health information that could be used to identify an individual	Written notification to affected individuals within 60 days; annual reporting to FTC unless 500 or more affected, in which case within 60 days; notice to "prominent media" within 60 days if 500 or more affected
Family Educational Rights and Privacy Act (FERPA) 34 CFR Part 99 Subpart D	Education records such as grades, transcripts, class lists, course schedules health records (for K-12 level), student financial aid information (for post-secondary level); student discipline files	Any public or private educational agency or institution that receives federal funding; any third party in receipt of education records from a public or private institution that receives federal funding	Disclosure of educational records or personal information derived from educational records without consent of guardian or student other than as permitted	FERPA requires an education agency or institution to maintain a record of every disclosure but does not require notification of affected individuals. FERPA's Safeguarding Recommendations, however, note that notification of affected individuals may be advisable, depending on the sensitivity of the compromised information.

Summary of Notification Laws				
Law	**Information covered**	**Applicability**	**Trigger**	**Notification requirements**
NYS Education Law Section 2d - Unauthorized release of personally identifiable information	Personally identifiable information (PII) from education records such as grades, transcripts, class lists, course schedules health records (for K-12 level), student financial aid information (for post-secondary level); student discipline files PII from professional performance reviews	NYS Dept. of Educ; NY school districts; boards of cooperative services (BOCES); schools; 3rd-party contractors providing services to the aforementioned	Unauthorized release of personally identifiable information derived from student records or principal/teacher performance records	Notification to the affected principal, teacher, parent, and/or "eligible student" (I.e., over 18 years old) of the unauthorized release of PII "in the most expedient way possible and without unreasonable delay." If the unauthorized release is attributable to a breach of security of a 3rd-party contractor, contractor will notify the educational agency "in the most expedient way possible and without unreasonable delay." The educational agency will notify the chief privacy officer of the NYS Dep't of Educ. Of the breach and the release of PII. Upon belief that such breach and unauthorized release constitutes criminal conduct, the chief privacy officer will notify law enforcement.

Sample Notification Letter

[Agency letterhead]

[Subject]

Dear [Name],

The [Agency] is writing to notify you to notify you of an incident regarding the privacy of some of your personal information. Although we are unaware of any actual or attempted misuse of your information, we are providing this notification out of an abundance of caution. This letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On [Date2], [description of incident].

What Information Was Involved? The information involved included [list all types of information affected].

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities. Upon discovering this incident, we moved quickly to investigate and took steps to prevent it from happening in the future. We are coordinating with the City's Chief Privacy Officer and the Office of Information Privacy to better understand and respond to the incident, and we are notifying you so that you may take further steps to help protect your personal information, should you feel it is appropriate to do so. Although we are unaware of any actual or attempted misuse of your information as a result of this incident, we are offering identity monitoring services through [vendor], for [timeframe], at no cost to you as an added precaution.

Additional information describing your services is included with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, review your account statements, and monitor your credit reports and explanation of benefits forms for suspicious activity and to detect errors. Please also review the enclosed "Steps You May Take To Help Protect Personal Information." You may also activate the free identity monitoring services available to you. The [Agency] will cover the cost of this service; but you will need to activate it yourself.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions, please contact us at [phone number]. Safeguarding your information is important to us, and the [Agency] remains committed to safeguarding the information in our care.

Sincerely,

[Agency signature]

Steps You May Take To Help Protect Personal Information

Activate Credit Monitoring

To help protect your identity, we are offering the services of [vendor] to provide identity monitoring at no cost to you for two years. [vendor] is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

> Visit [URL] to activate your credit monitoring services. You have until [Date2] to activate your credit monitoring services. Your membership number is [Member ID].

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a [vendor] fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a [vendor] fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced [vendor] licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Monitor Your Accounts

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, **1-877-322-8228**. You may also contact the three major credit bureaus listed below directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who

gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**Transunion**	**Equifax**
PO Box 9554	PO Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**Transunion**	**Equifax**
PO Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	PO Box 2000 Chester, PA 19016 1-888-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	PO Box 105069 Atlanta, GA 30348 1-800-685-1111 www.equifax.com/personal/credit-report-services

Additional Steps You May Take

Strengthen Your Account Security

Cybercriminals sometimes use exposed account related information to gain unauthorized access, leading to the potential for identity theft, financial loss, and other privacy issues. **Changing your passwords immediately** for affected accounts and any others that use the same password helps to prevent unauthorized access.

To further protect against potential threats to your login information, consider **updating your passwords according to best practices** from the Cybersecurity and Infrastructure Security Agency, ensuring sure your password is:

- At least 16 characters, but longer if possible
- A random string of mixed letters OR;
- A memorable phrase of 4 – 7 unrelated words
- A combination of uppercase letters, lowercase letters, numbers, and symbols
- Significantly different from your previous passwords
- Memorized or stored in a password manager

Adding Two-Factor Authentication adds an additional layer of security, making it significantly harder for attackers to compromise your accounts through exposed passwords by requiring a second form of verification.

Watch for Signs of Identity Theft

In addition to utilizing the credit monitoring offered in this letter, you should watch for signs that your information was potentially exploited, including:

- Being locked out of your accounts
- Transactions you don't recognize on account statements
- Unexpected notifications
- Unusual activity on your social security account
- Unsolicited password reset notifications
- New account sign ups you didn't initiate
- Unexpected bills or statements
- Unusual drops in your credit score
- Your tax return is rejected
- Debt collectors call you

Don't be Tricked by Scammers using the Exposed Data

In the aftermath of a data breach, scammers sometimes exploit the situation by contacting impacted individuals under false pretenses. Be wary of unsolicited emails, texts, or phone calls that contact you under a pretext that involves information exposed in a breach. Don't believe anyone who calls and says

you'll be arrested unless you pay for taxes or debt – even if they have part of or your entire Social Security number, or they say they're from the IRS.

Consider How Else the Exposed Information Might Affect You Personally

Each person's life circumstances are different, and the impact of disclosed information can vary widely. For instance, if you are in a vulnerable position, such as being a survivor of domestic violence or stalking, the disclosure of your address or contact information can pose a safety risk. In such cases, consider reaching out to local support organizations such as NYC Hope at [redacted] or online at **https://www.nyc.gov/content/nychope/pages/** and contact law enforcement for guidance on additional protective measures.

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect your minor by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at:

600 Pennsylvania Avenue NW
Washington, DC 20580
www.identitytheft.gov
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261.

The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

For New York residents, the Attorney General may be contacted at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov.

Instructions for Accessing the Citywide Breach Notification and Credit Monitoring Contract

The Office of Technology and Innovation obtained secure credit monitoring and breach notification services through Identity Theft Guard Solutions, doing business as IDX. City agencies can use OTI's contract for their own credit monitoring and breach needs.

1. Access the listing of Citywide IT General Contracts.
    a. Non-Mayoral agencies may not be able to access the listing. Contact the Office of Information Privacy if you are not able to access the listing.
2. Download and familiarize yourself with the Citywide Breach Notification and Credit Monitoring Solutions contract and Breach Notification - Credit Order form.
3. Contact Office of Technology and Innovation at oip@oti.nyc.gov, [redacted], and [redacted] and provide background as to the proposed utilization to ensure Office of Technology and Innovation approval of the utilization.
4. Contact IDX [redacted] and IDX [redacted] to begin a dialogue regarding services (while being mindful always to include your agency's general counsel on any communications).
    a. IDX will request details as to the incident which gave rise to the need for credit monitoring and breach notification services.
    b. IDX will prepare a statement of work and a quote. Review the statement of work and quote to ensure that it meets your needs. The pricing provided should track the rates set forth in the contract on pages 272-273.
5. Obtain internal approvals (such as from your agency chief contracting officer) and complete the Breach Notification - Credit Order Form using information from the approved statement of work and quote.
6. Submit the completed and signed Breach Notification Order Form, statement of work and quote, and Citywide Breach Notification and Credit Monitoring Solutions contract to IDX and your agency chief contracting officer, with your agency's general counsel copied.
7. IDX will begin services and will invoice your agency directly throughout the service period.

Contracts and Agreements

Instructions

This section provides guidance on privacy protection in contracting and implementing the requirements of the Citywide Privacy Protection Policies and Protocols Section 6. The Citywide Privacy Protection Policies and Protocols are binding on all agencies subject to the Identifying Information Law as well as contractors for human services, technology services involving sensitive identifying information, and outreach services involving the identifying information of another agency.

The section also includes sample privacy protection terms that agencies can add to contracts that are not covered by the Identifying Information Law, and template agreements for interagency data sharing agreements, external nondisclosure agreements, and agreements with oversight agencies. Consult with agency counsel on incorporating these documents into agency practices.

Crosswalk of IIL Requirements and Guidance on Privacy Attachments		
	Coverage	**Description**
(1)	Contracts and subcontracts for human services. **Attach Identifying Information Rider**	• Services provided to third parties, including social services such as day care, foster care, home care, homeless assistance, housing and shelter assistance, preventive services, youth services, and senior centers; health or medical services including those provided by health maintenance organizations; legal services; employment assistance services, vocational and educational programs; and recreation programs.
(2)	Contracts and subcontracts for technology services involving sensitive identifying information. **Attach Identifying Information Rider**	• Technology or technology services procured by the City are used by the contractor or subcontractor on behalf of the City to collect, access, store, process, analyze, transmit, or otherwise handle sensitive identifying information, or which make sensitive identifying information accessible to the contractor even if access is not the express purpose of the contract. ***NOTE: This designation excludes the following types of contracts:*** • Contracts where the vendor simply provides a technology product to the City, such as basic computer hardware or on-premises software which does not involve the vendor's access to sensitive identifying information. • Subcontracts for technology services that generally govern the subcontractor's business relationships as a whole (i.e., for a broad range of clients, and not just specifically the City), provided that the City contractor includes appropriately protective privacy and security provisions in such subcontracts.
(3)	Contracts and subcontracts for outreach services involving identifying information. **Attach Identifying Information Rider**	• Contractor or subcontractor collects, uses, discloses, or accesses identifying information (except for routine business contact information) on behalf of the City for projects designed to help clients of other City agencies or offices (or members of the public) access information about City services, resources, or events, through any means.

Crosswalk of IIL Requirements and Guidance on Privacy Attachments		
(4)	Effective dates and requirements for covered contracts. **Attach Identifying Information Rider**	• All contracts and subcontracts for human services **entered into or renewed on or after June 15, 2018**, are subject to the Identifying Information Law. • Contracts and subcontracts for technology or technology services involving sensitive identifying information and contracts and subcontracts for outreach services involving identifying information **entered into or renewed on or after July 1, 2021**, are subject to the Identifying Information Law.
(5)	Contracts for sensitive identifying information that are not covered contracts under the Identifying Information Law. **Attach Privacy Protection Rider or include appropriate privacy provisions**	• Contracts of any value involving the vendor's collection, use, disclosure, or access of sensitive identifying information that are not covered contracts.

Checklist: Privacy Requirements for Contracts with Non-City Parties			
This checklist can be used to help determine which privacy-related terms, attachments, and requirements apply to City agency agreements with non-City entities.			
	Requirement	**Description**	**Completed**
(1)	Obtain agency privacy officer approval for all collections, uses, or disclosures of identifying information involving non-City parties.	• The agency privacy officer must approve any collection, use, disclosure, or access of identifying information to any party. NOTE: This requirement also applies to collections, uses, disclosures, or access between City parties.	☐
(2)	If an agreement involves disclosure of identifying information to an external (non-City) party, obtain Law Department review.	• Consult the Law Department's Contracts Division when an agreement involves disclosure of identifying information to a non-City party, unless the Law Department advises otherwise.	☐
(3)	If a contract or subcontract is covered by Identifying Information Law, attach the Identifying Information Rider.	• The Identifying Information Law expressly applies to contractors and subcontractors for "human services."	☐

(4)	If Chief Privacy Officer has designated the type of contract or subcontract as subject to the Identifying Information Law's requirements, attach the Identifying Information Rider.	• Contract is entered into or renewed on or after July 1, 2021, *and* is either: ○ A contract or subcontract in which the contractor's or subcontractor's technology or technology services are procured by the City and used by the contractor or subcontractor on behalf of the City to collect, access, store, process, analyze, transmit, or otherwise handle sensitive identifying information, or which make sensitive identifying information accessible to the contractor or subcontractor in connection with such contract or subcontract although such access may not be the express purpose of the contract, *or* ○ A contract or subcontract where the contractor or subcontractor collects, uses, discloses, or accesses identifying information (except for routine business contact information) on behalf of the City for projects designed to help clients of other City agencies or offices (or members of the public) access information about City services, resources, or events, through any means.	☐
(5)	If a contract or subcontract involves sensitive identifying information but is not a covered contract, agencies should include appropriate privacy terms or attach the Privacy Protection Rider.	• Contracts involving use of "sensitive identifying information" (defined in Citywide Privacy Protection Policies and Protocols § 3.2.10) should either: ○ attach the Privacy Protection Rider, or ○ include terms protecting the privacy of the information. NOTE: Contracts may include both the Privacy Protection Rider *and* additional privacy terms.	☐
(6)	If a contract or subcontract is between an agency and a vendor that will perform outreach to the agency's own clients, agencies may attach the Privacy Protection Rider.	• Agencies are encouraged to attach the Privacy Protection Rider to these contracts.	☐

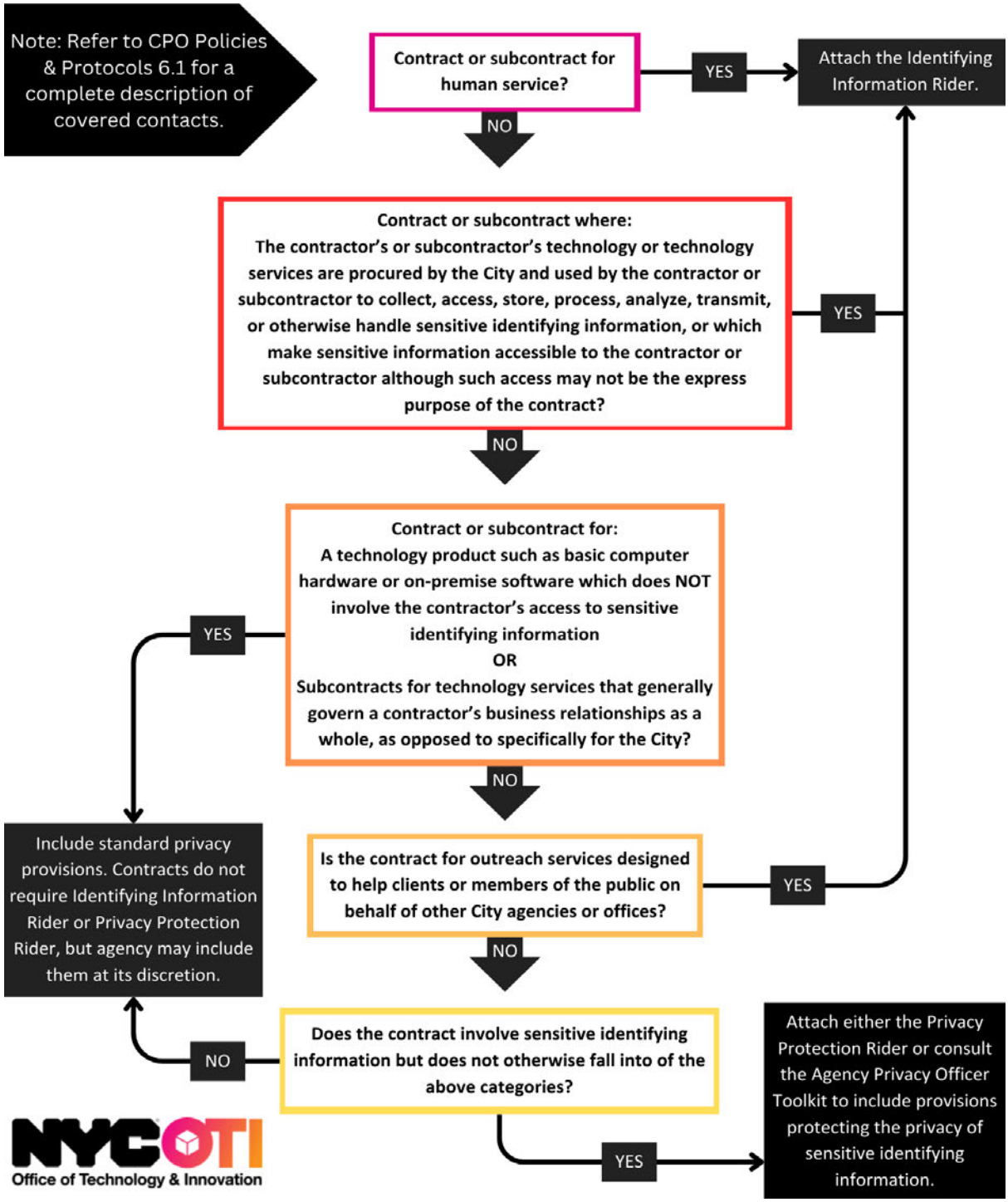
(7)	Confirm that all relevant privacy and security attachments are included in the contract.	• Refer to the Guidance for Privacy Attachments to determine if other applicable privacy and security terms, riders, attachments, and appendices should be attached to the contract. The Guidance for Privacy Attachments includes documents required by the Law Department and the City's Office of Technology and Innovation.	☐

Contracts Compliance At-A-Glance: IIL and CPO Policies and Protocols			
	Description	**Requirement**	**Completed**
(1)	Is the contract for human services for any value?	If **YES**: Attach the Identifying Information Rider. If **NO**: Go to (2).	☐
(2)	Is the contract: • A contract or subcontract for technology or technology services in which the contractor's or subcontractor's technology or technology services are procured by the City and used by the contractor or subcontractor on behalf of the City to collect, access, store, process, analyze, transmit, or otherwise handle sensitive identifying information, or which makes sensitive identifying information accessible to the contractor or subcontractor in connection with such contract or subcontract although such access may not be the express purpose of the contract?	If **YES**: Attach the Identifying Information Rider. If **NO**: Go to (3).	☐

(3)	Is the contract: • A contract where the vendor simply provides a technology product to the City, such as basic computer hardware or on-premise software which does not involve the vendor's access to sensitive identifying information, **OR** • A subcontract for technology services that generally governs a contractor's business relationships as a whole (i.e., for a broad range of clients, and not just specifically the City), provided that the City contractor includes appropriately protective privacy and security provisions in such subcontracts?	If **YES:** These contracts do not require the Identifying Information Rider or Privacy Protection Rider, but agency may include them at its discretion. Include standard privacy protection terms (refer to the Sample External Non-Disclosure Agreement for examples). If **NO**: Go to (4).	☐
(4)	Is the contract a contract or subcontract where the contractor or subcontractor collects, uses, discloses, or accesses identifying information (except for routine business contact information) on behalf of the City for projects designed to help clients of other City agencies or offices (or members of the public) access information about City services, resources, or events, through any means?	If **YES**: Attach the Identifying Information Rider. If **NO**: Go to (5).	☐

(5)	Does the contract involve sensitive identifying information but not otherwise fall into one of the above categories?	If **YES**: Attach either the Privacy Protection Rider or consult the Guidance for Drafting Contract Terms to Protect Sensitive Identifying Information. If **NO**: Include standard privacy protection terms (refer to the Sample External Non-Disclosure Agreement for examples).	☐

Contract Flowchart on Privacy Attachments



Checklist: Non-Covered Contracts and Subcontracts			
This section applies to contracts or subcontracts that are not subject to the Identifying Information Law because they are not covered contracts, meaning they are not contracts for human services and they are not contracts for services designated by the Chief Privacy Officer as being subject to the Identifying Information Law's requirements.			
	Scenario	**Requirements**	**Completed**
(1)	Contractor or subcontractor will collect, use, disclose, or access identifying information.	The agency privacy officer must approve the collection, use, disclosure, or access of identifying information.	☐
(2)	Contractor or subcontractor will collect, use, disclose, or access sensitive identifying information.	The contract should include: • Description of information to be treated as sensitive identifying information • Specification of which users will have access to the sensitive identifying information • The purpose for accessing the sensitive identifying information • The standard of care for protecting the sensitive identifying information • Security measures that individuals with access will follow when handling the sensitive identifying information • Requirement to cooperate with City investigations into unauthorized disclosures Contracts for professional services involving access to City technology or City data should include Office of Technology and Innovation Attachment SCY. If the agreement does not include Office of Technology and Innovation Attachment SCY, it should include protocols that explain how to handle suspected or known data security incidents, including: • Protocols and timeframes for notifying external parties • Efforts to mitigate harm from disclosure • Safeguards against redisclosure	☐

(3)	Contractor or subcontractor will retain sensitive identifying information.	The contract should include: • Duration of the retention • Language specifying that the contractor or subcontractor must keep the sensitive identifying information confidential, unless disclosure is authorized by the contract or required by law • Language specifying that the confidentiality of the information will outlast the contract's termination • Language specifying requirements for data destruction or return	☐
(4)	Contractor or subcontractor seeks to access or use sensitive identifying information for purposes beyond those agreed to in the contract.	If the agency (including the agency privacy officer, in writing) **approves** the additional use, the contract should be revised or supplemented with language specifying: • Each data element to be accessed or used • Purpose of the use • Individuals or groups that will access or use the information • How the information will contribute to the use • How the information will be returned or destroyed If the agency **restricts or prohibits** the access or use, the contract must clearly state such restrictions or prohibitions.	☐
(5)	Contractor or subcontractor seeks to sell or otherwise monetize sensitive identifying information.	The contract **must** contain language prohibiting the sale, disclosure, or use of such information for the contractor's or subcontractor's own benefit or that of another, unless expressly authorized by the contract. **Agencies should consult with the Chief Privacy Officer before authorizing sale, disclosure, or use of such information.**	☐

Guidance for Relevant Privacy Attachments

Note: Some agreements may require multiple attachments.

Type of City Contract	Attachment
Is this a contract for any consultant, professional, technical, human, and/or client services, valued at $100,000 or above?	Law Department Appendix A must be attached, except for certain types of contracts, including: purchases from State or federal contracts; contracts with a governmental entity; preferred source contracts; or contracts where the Law Department uses Rider 1 instead. (For further information on these and other exceptions, reach out to agency counsel or contact the Law Department.)
Is this a human services contract of any value?	Identifying Information Rider must be attached.
Is this a contract of any value for services that the Chief Privacy Officer has formally designated as being subject to the requirements of the Identifying Information Law (i.e., technology services involving sensitive identifying information or certain outreach services involving identifying information) ("covered contracts")?[23]	Identifying Information Rider must be attached.
Does this contract require additional privacy protections because: (1) the contract involves the collection, use, disclosure of, or access to sensitive identifying information of members of the public or City employees or officials; or (2) the nature of the identifying information and the circumstances of its collection or potential disclosure by Contractor implicates an important privacy risk?	Privacy Protection Rider should be attached.

[23] Refer to Crosswalk of IIL Requirements and CPO Guidance on Privacy Attachments for definitions and additional guidance about these designated services.

Does this contract include the collection, use, disclosure of, or access to identifying information that is protected by a New York State or federal law? (Or, if applicable to the transaction, another state's laws?)	Incorporate appropriate privacy and data security provisions into the contract. Adjust these provisions as needed to ensure compliance with relevant federal or state laws and regulations.
Does this contract involve the purchase, lease, or licensing of cloud-based technology services such as Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), or Platform-as-a-Service (PaaS), or any other cloud services where access to City data is involved, regardless of whether identifying information is present?	Office of Technology and Innovation's Cloud Services Agreement must be attached. Consult with Office of Technology and Innovation, Office of the General Counsel at [redacted].
Is the contract for the purchase of professional services involving access to City technology or City data?	OTI's Attachment SCY must be attached. Consult with OTI Office of the General Counsel at [redacted].

Required Data Sharing Agreements Between City Agencies

Agencies must obtain agency privacy officer approval for all collection, use, disclosure, access to, and retention of identifying information outside of the agency. In addition, if any of the following circumstances apply to an agency's disclosure of identifying information, a data sharing agreement is required when:

- The agency is making non-routine disclosures of identifying information to another City agency. This applies unless the disclosure is made under exigent circumstances, or if the agency privacy officer has consulted the Chief Privacy Officer and determined an agreement is not necessary (Citywide Privacy Protection Policies and Protocols § 6.2.1).
- The agency is disclosing sensitive identifying information, whether such disclosure is routine or non-routine. (Citywide Privacy Protection Policies and Protocols §§ 3.2.10, 5.0, and 6.2.1.)
- The agency is disclosing identifying information that is restricted by other laws or regulations.
- The agency is transferring custody and maintenance of identifying information to a third party, including another City agency.
- Disclosures to a third-party may require additional contractual protections, such as but not limited to insurance, intellectual property and ownership, and indemnification.

Refer to Citywide Privacy Protection Policies and Protocols §§ 6.2.1 and 6.2.2 for additional guidance on how to draft such data sharing agreements.

Identifying Information Rider 3.0

1. Purpose.

Contractor agrees to comply with this Identifying Information Rider ("Rider") and the Identifying Information Law, as applicable, in the performance of this Agreement.

2. Definitions.

A. "Access" to Identifying Information means gaining the ability to read, use, copy, modify, process, or delete any information whether or not by automated means.

B. "Agency" means a City agency or office through which the City has entered into this Agreement.

C. "Authorized Users" means employees, officials, subcontractors, or agents of Contractor whose collection, use, disclosure of, or access to Identifying Information is necessary to carry out the Permitted Purpose.

D. "Chief Privacy Officer" means the City's Chief Privacy Officer.

E. "Collection" means an action to receive, retrieve, extract, or access Identifying Information. Collection does not include receiving information that Contractor did not ask for.

F. "Contractor" means an entity entering into this Agreement with the City.

G. "Disclosure" means releasing, transferring, disseminating, giving access to, or otherwise providing Identifying Information in any manner outside Contractor. Disclosure includes accidentally releasing information and access to Identifying Information obtained through a potential unauthorized access to Contractor's systems or records.

H. "Exigent Circumstances" means cases where following this Rider would cause undue delays.

I. "Identifying Information" means any information provided by the City to Contractor or obtained by Contractor in connection with this Agreement that may be used on its own or with other information to identify or locate an individual.

J. "Identifying Information Law" means §§ 23-1201 – 1205 of the Administrative Code of the City of New York.

K. "Permitted Purpose" means a use of Identifying Information that is necessary to carry out Contractor's obligations under this Agreement.

L. "Use" of Identifying Information means any operation performed on Identifying Information, whether or not via automated means, such as collection, storage, transmission, consultation, retrieval, disclosure, or destruction.

3. General Requirements.

A. Contractor will use appropriate physical, technological, and procedural safeguards to protect Identifying Information.

B. Contractor will restrict collection, use, disclosure of, or access to Identifying Information to Authorized Users for a Permitted Purpose.

C. Contractor will comply with the Citywide Cybersecurity Requirements for Vendors and Contractors set forth by the New York City Office of Technology and Innovation and its Office of Cyber Command as they appear at https://nyc.gov/infosec. Contractor will ensure that Authorized Users understand and comply with the provisions of this Agreement applicable to Identifying Information.

D. Contractor and Authorized Users will not use Identifying Information for personal benefit or the benefit of another, nor publish, sell, license, distribute, or otherwise reveal Identifying Information outside the terms of this Agreement.

4. Collection.

A. Absent Exigent Circumstances (Section 7.0), Contractor may collect Identifying Information if the collection:

i. has been approved by the agency privacy officer;

ii. is required by law or treaty;

iii. is required by the New York City Police Department in connection with a criminal investigation; or

iv. is required by a City agency in connection with an open investigation concerning the welfare of a minor or an individual who is not legally competent.

5. Disclosure.

A. Absent Exigent Circumstances (Section 7.0), Contractor may disclose Identifying Information if the disclosure:

i. has been approved by the agency privacy officer;

ii. is required by law or treaty;

iii. is required by the New York City Police Department in connection with a criminal investigation; or

iv. is required by a City agency in connection with an open investigation concerning the welfare of a minor or an individual who is not legally competent; or

v. has been authorized in writing by the individual to whom such information pertains or, if the individual is a minor or is otherwise not legally competent, by the individual's parent, legal guardian, or other person with legal authority to consent on behalf of the individual.

6. Disclosures of Identifying Information to Third Parties.

Unless prohibited by law, Contractor will promptly notify the agency privacy officer of any third-party requests for Identifying Information, cooperate with the agency privacy officer to handle such requests, and comply with the Chief Privacy Officer's policies and protocols concerning requirements for a writtenagreement governing the disclosure of Identifying Information to a third party.

7. Exigent Circumstances.

A. Notwithstanding Section 4.0 (Collection) and 5.0 (Disclosure), if Contractor collects or discloses Identifying Information due to Exigent Circumstances, then as soon as practicable after the collection or disclosure but not to exceed 24 hours, Contractor will send to the agency privacy officer in writing:

i. The name, e-mail address, phone number, and title of a Contractor point of contact with sufficient knowledge and authority who will respond promptly to and collaborate with the agency privacy officer;

ii. A description of the Exigent Circumstances, including a detailed timeline, all involved parties, the types of Identifying Information disclosed or collected, and Contractor's estimate of the likelihood of the Exigent Circumstances reoccurring.

B. If the agency privacy officer determines the collection or disclosure was not made under Exigent Circumstances, the collection or disclosure will be deemed in violation of this Rider and subject to the provisions of Section 8(A)-8(D).

8. Unauthorized Collection, Use, Disclosure of, or Access to Identifying Information.

A. If Contractor collects, discloses, uses, or accesses Identifying Information in violation of this Rider, Contractor will:

i. notify the agency privacy officer in writing as soon as practicable but no later than 24 hours after discovery, including a description of the collection, disclosure, use, or access, the types of Identifying Information that may have been involved or compromised, the names and affiliations of the parties (if known) who gained access to Identifying Information without authorization, and a description of the steps taken, if any, to mitigate the effects of the collection, disclosure, use, or access incident;

ii. cooperate with the agency privacy officer and relevant City officials, including the City's Chief Privacy Officer, Office of Cyber Command, and the City's Law Department, to investigate the occurrence and scope of the collection, disclosure, use, or access, and make any required or voluntary notices; and,

iii. take all necessary steps, as determined by the agency privacy officer, to prevent or mitigate the effects of the collection, disclosure, use, or access.

B. If there is an alleged collection, use, disclosure, or access violation, the Agency may investigate the alleged violation. Contractor will cooperate with the investigation, which may include prompt:

i. provision to the City of information related to security controls and processes, such as third-party certifications, policies and procedures, self-assessments, independent evaluations and audits, view-only samples of security controls, logs, files, incident reports or evaluations;

ii. verbal interviews of individuals with knowledge of Contractor's security controls and processes or the unauthorized collection, use, disclosure, or access;

iii. an evaluation or audit by the City of Contractor's security controls and processes, and the unauthorized collection, use, disclosure, or access;

iv. an evaluation or audit by Contractor of its security controls and processes and the unauthorized collection, use, disclosure, or access, and provision of any attendant results to the City; or,

v. an independent evaluation or audit to be provided to the City of Contractor's security controls and processes, and the unauthorized collection, use, disclosure, or access.

C. If the agency privacy officer or Chief Privacy Officer determines that notification to affected individuals is required pursuant to the policies and protocols promulgated by the Chief Privacy Officer under subdivision 6 of Section 23-1203, then the agency privacy officer will inform Contractor whether the Agency or the Contractor will issue the notification. If the agency privacy officer directs Contractor to issue the notification, the notification will be issued in writing as soon as practicable and will conform to the agency privacy officer's instructions as to form, content, scope, and recipients.

D. Monies and Set-Off.

i. Contractor will pay for services deemed necessary by the agency privacy officer to address Contractor's collection, disclosure, use, or access of Identifying Information in violation of this Rider, subject to limitations of liability contained elsewhere in this Agreement. These services may include: (a) credit monitoring services; (b) notifications; (c) payment of any fines or disallowances imposed by the State or federal government related to a collection, use, disclosure, or access in violation of this Rider; (d) other actions mandated by any law, administrative or judicial order, agency privacy officer, or the Chief Privacy Officer.

ii. At the agency privacy officer's discretion, the Agency may pay for services deemed necessary to address Contractor's collection, disclosure, use, or access of Identifying Information in violation of this Rider. If the Agency pays for any of these services, it may submit invoices to Contractor and Contractor will promptly reimburse the Agency.

iii. If Contractor refuses to pay for services deemed necessary by the agency privacy officer, the City may, for the purpose of set-off in sufficient sums without waiver of any other rights and remedies:

a. withhold further payments under this Agreement to cover the costs of notifications and other actions mandated by any law, administrative or judicial order, agency privacy officer, or the Chief Privacy Officer, including any related fines or disallowances imposed by the State or federal government;

b. withhold further payments to cover the costs of credit monitoring services, and any other commercially reasonable preventive measures;

c. instruct Contractor to pay directly for the services detailed in this subsection 8(C)(iii)(a) and 8(C)(iii)(b) using monies remaining to be earned under this Agreement.

E. Contractor is not required to make any notification that would compromise public safety, violate any law, or interfere with a law enforcement investigation or other investigative activity by the Agency.

9. Retention.

Contractor will retain Identifying Information as required by law or as otherwise necessary in furtherance of this Agreement, or as otherwise approved by the agency privacy officer.

10. Reporting.

Contractor will provide the Agency with reports as requested by the agency privacy officer or Chief Privacy Officer regarding Contractor's collection, retention, disclosure of, and access to Identifying Information. Each report will includeinformation concerning Identifying Information collected, retained, disclosed, and accessed including: (a) the types of Identifying Information collected, retained, disclosed, or accessed; (b) the types of collections and disclosures classified as "routine" and any collections or disclosures approved by the agency privacy officer or Chief Privacy Officer; and (c) any other related information that may be reasonably required by the agency privacy officer or Chief Privacy Officer.

11. Auditing.

A. No less than once per year, Contractor shall conduct a comprehensive audit of its privacy program and provide its findings to the Agency.

B. In addition to the auditing required by subsection 11(A), Contractor shall engage a third-party internationally recognized auditor, at Contractor's own cost, to perform periodic audits, scans, and tests, and audit as follows at least once per year and after Contractor collects, discloses, uses, or accesses Identifying Information in violation of this Rider and at the request of the Agency:

   i. a verification of Contractor's compliance with the provisions of this Rider and laws governing Identifying Information;

   ii. an assessment of Contractor's privacy practices against recognized industry best practices, and including a gap analysis identifying areas where Contractor's practices fall short of industry best practices and recommending improvements, including assessments of:

      a. the necessity the amounts and types of Identifying Information collected;
      b. the adequacy of retention and deletion policies;
      c. subject rights management;
      d. accuracy and understandability of internal and external privacy policies;

iii. a privacy risk assessment, prioritizing areas of highest risk to Identifying Information, producing a risk profile and suggested mitigation strategies for any material vulnerabilities identified.

C. The Agency may review and audit Contractor's privacy program prior to the commencement of this Agreement and from time to time during the term of this Agreement. Contractor shall allow the Agency to perform audits, and shall fully cooperate and furnish all requested materials in a timely manner. Audits may be conducted by the Agency or an Agency provider and at the Agency's expense. At the Agency's option, Contractor shall complete, within 45 days of receipt, an audit questionnaire provided by the Agency regarding Contractor's privacy program. Contractor shall not be entitled to compensation from the Agency for the time it spends cooperating with any of the audits, scans, or tests provided for in this Section.

12. Coordination with agency privacy officer.

The Agency may assign powers and duties of the agency privacy officer to Contractor for purposes of this Agreement. Insuch event, Contractor will exercise those powers and duties in accordance with applicable law in relation to this Agreement and will comply with directions of the agency privacy officer and Chief Privacy Officer concerning coordination and reporting.

13. Destruction of Identifying Information.

If the Agency instructs Contractor to destroy Identifying Information, Contractor will destroy it within 30 days after receiving the instruction in a way that it cannot be reconstructed, subject to any litigation holds. Contractor will provide written confirmation to the agency privacy officer that it has destroyed the Identifying Information within 30 days after receiving the instruction. If it is impossible for Contractor to destroy the Identifying Information, Contractor will promptly explain in writing why it is impossible, and will, upon receiving the destruction request, immediately stop accessing or using the Identifying Information, and will maintain such Identifying Information in accordance with this Rider.

14. Subcontracts.

A. Contractor will include this Rider in all subcontracts to provide human services or other services designated inthe policies and protocols of the Chief Privacy Officer.

B. Contractor will be responsible to the Agency for compliance with this Rider by its subcontractors that provide human services or other services designated by the Chief Privacy Officer.

15. Conflicts with Provisions Governing Records and Reports.

To the extent allowed by law, the provisions of this Rider will control if there is a conflict between any of its provisions and, as applicable, either (a) Article 5 of Appendix A (General Provisions Governing Contracts for Consultants, Professional, Technical, Human, and Client Services); (b) if the value of this Agreement is $100,000 or less and is funded by City Council Discretionary Funds, Article 7(E) and Rider 1, Article 1 of this Agreement; or (c) if neither (a) nor (b) apply, the other provisions concerning records retention and reports designated elsewhere in this Agreement. The provisions of this Rider do not replace or supersede any other obligations or requirements of this Agreement.

Privacy Protection Rider

1. Purpose.

The agency privacy officer has determined that an important privacy risk is implicated by the services provided under this Agreement. Contractor agrees to comply with this Privacy Protection Rider ("Rider") and the Identifying Information Law, as applicable, in the performance of this Agreement.

2. Definitions.

A. "Access" to Identifying Information means gaining the ability to read, use, copy, modify, process, or delete any information whether or not by automated means.

B. "Agency" means a City agency or office through which the City has entered into this Agreement.

C. "Authorized Users" means employees, officials, subcontractors, or agents of Contractor whose collection, use, disclosure of, or access to Identifying Information is necessary to carry out the Permitted Purpose.

D. "Chief Privacy Officer" means the City's Chief Privacy Officer.

E. "Collection" means an action to receive, retrieve, extract, or access Identifying Information. Collection does not include receiving information that Contractor did not ask for.

F. "Contractor" means an entity entering into this Agreement with the City.

G. "Disclosure" means releasing, transferring, disseminating, giving access to, or otherwise providing Identifying Information in any manner outside Contractor. Disclosure includes accidentally releasing information and access to Identifying Information obtained through a potential unauthorized access to Contractor's systems or records.

H. "Exigent Circumstances" means cases where following this Rider would cause undue delays.

I. "Identifying Information" means any information provided by the City to Contractor or obtained by Contractor in connection with this Agreement that may be used on its own or with other information to identify or locate an individual.

J. "Identifying Information Law" means §§ 23-1201 – 1205 of the Administrative Code of the City of New York.

K. "Permitted Purpose" means a use of Identifying Information that is necessary to carry out the Contractor's obligations under this Agreement.

L. "Sensitive Identifying Information" means Identifying Information that poses a higher risk of harm to an individual or members of an individual's household. Examples of harm are identity theft, danger to health and safety, severe financial loss, reputational harm, or other harms dependent upon any protected status of an individual.

M. "Use" of Identifying Information means any operation performed on Identifying Information, whether or not via automated means, such as collection, storage, transmission, consultation, retrieval, disclosure, or destruction.

3. General Requirements.

A. Contractor will use appropriate physical, technological, and procedural safeguards to protect the security of Identifying Information and will take reasonable measures to prevent harm to the City and the individuals whose Identifying Information is subject to this Agreement.

B. Contractor will restrict collection, use, disclosure of, or access to Identifying Information to Authorized Users for a Permitted Purpose.

C. Contractor will comply with the Citywide Cybersecurity Requirements for Vendors and Contractors set forth by the New York City Office of Technology and Innovation and its Office of Cyber Command as they appear at https://nyc.gov/infosec. Contractor will ensure that Authorized Users understand and comply with the provisions of this Agreement applicable to Identifying Information.

D. Contractor and Authorized Users will not use Identifying Information for personal benefit or the benefit of another, nor publish, sell, license, distribute, or otherwise reveal Identifying Information outside the terms of this Agreement.

4. Collection.

A. Absent Exigent Circumstances (Section 7), Contractor may collect Identifying Information if the collection:

i. has been approved by the agency privacy officer;

ii. is required by law or treaty;

iii. is required by the New York City Police Department in connection with a criminal investigation; or

iv. is required by a City agency in connection with an open investigation concerning the welfare of a minor or other individual who is not legally competent.

5. Disclosure.

A. Absent Exigent Circumstances (Section 7), Contractor may disclose Identifying Information if the disclosure:

i. has been approved by the agency privacy officer;

ii. is required by law or treaty;

iii. is to the New York City Police Department in connection with a criminal investigation;

iv. is required by a City agency in connection with an open investigation concerning the welfare of a minor or an individual who is not legally competent; or

v. has been authorized in writing by the individual to whom such information pertains or, if such individual is a minor or is otherwise not legally competent, by such individual's parent, legal guardian, or other person with legal authority to consent on behalf of the individual.

B. If Contractor is required by law to disclose Identifying Information, it will: (a) as soon as practicable, but not later than one business day after it learns of the required disclosure, notify the Agency; and (b) disclose the Identifying Information only to the extent allowed under a protective order or as necessary to comply with the law.

6. Disclosures of Identifying Information to Third Parties.

Unless prohibited by law, Contractor will promptly notify the agency privacy officer of any third-party requests for Identifying Information, cooperate with the agency privacy officer to handle such requests, and comply with the Citywide Privacy Protection Protocols of the Chief Privacy Officer concerning requirements for a written agreement governing the disclosure of Identifying Information to a third party.

7. Exigent Circumstances.

A. Notwithstanding Section 4.0 (Collection) and 5.0 (Disclosure), if Contractor collects or discloses Identifying Information due to Exigent Circumstances with no other basis for collection or disclosure under subdivisions (b) or (c) of Section 23-1202, then as soon as practicable after the collection or disclosure but not to exceed 24 hours, Contractor will send to the agency privacy officer in writing:

i. The name, e-mail address, phone number, and title of a Contractor point of contact with sufficient knowledge and authority who will respond promptly to and collaborate with the agency privacy officer;

ii. A description of the Exigent Circumstances, including a detailed timeline, all involved parties, the types of Identifying Information disclosed or collected, and Contractor's estimate of the likelihood of the Exigent Circumstances reoccurring.

B. If the agency privacy officer determines the collection or disclosure was not made under Exigent Circumstances, the collection or disclosure will be deemed in violation of this Rider and subject to Section 8 (Unauthorized Collection, Use, Disclosure of, or Access to Identifying Information).

8. Unauthorized Collection, Use, Disclosure of, or Access to Identifying Information.

A. If Contractor collects, uses, discloses, or accesses Identifying Information in violation of this Rider, Contractor will:

i. notify the agency privacy officer in writing as soon as practicable but no later than 24 hours after discovery, including a description of the collection, disclosure, use, or access, the types of Identifying Information that may have been involved or compromised, the names and affiliations of the parties (if known) who gained access to Identifying Information without authorization, and a description of the steps taken, if any, to mitigate the effects of the collection, disclosure, use, or access;

ii. provide the name, e-mail address, phone number, and title of a Contractor point of contact with sufficient knowledge and authority who will respond promptly to and collaborate with the agency privacy officer and relevant City officials, including the Chief Privacy Officer, Office of Cyber Command, and the City's Law Department, to investigate the occurrence and scope of the collection, disclosure, use, or access, and make any required or voluntary notices;

iii. take all reasonably necessary steps, as determined by the agency privacy officer, to prevent or mitigate the effects of the unauthorized collection, use, disclosure, or access.

B. If there is an alleged collection, use, disclosure, or access violation, the Agency may investigate the alleged violation. Contractor will cooperate with the investigation, which may include prompt:

i. provision to the City of information related to security controls and processes, such as third-party certifications, policies and procedures, self-assessments, independent evaluations and audits, view-only samples of security controls, logs, files, incident reports or evaluations;

ii. verbal interviews of individuals with knowledge of Contractor's security controls and processes or the unauthorized collection, use, disclosure, or access;

iii. an evaluation or audit by the City of Contractor's security controls and processes, and the unauthorized collection, use, disclosure, or access;

iv. an evaluation or audit by Contractor of its security controls and processes and the unauthorized collection, use, disclosure, or access, and provision of any attendant results to the City; or,

v. an independent evaluation or audit to be provided to the City of Contractor's security controls and processes, and the unauthorized collection, use, disclosure, or access.

C. If the agency privacy officer or the Chief Privacy Officer determine that an unauthorized collection, use, disclosure, or access requires notification to individuals pursuant to any law or the policies and protocols promulgated by the Chief Privacy Officer under subdivision 6 of Section 23-1203, then the agency privacy officer will inform Contractor whether the Agency or the Contractor will issue the notification. If the agency privacy officer directs Contractor to issue the notification, the notification will be issued in writing as soon as practicable and will conform to the agency privacy officer's instructions as to form, content, scope, and recipients.

D. Monies and Set-off.

i. Contractor will pay for services deemed necessary by the agency privacy officer to address the collection, use, disclosure, or access to Identifying Information in violation of this Rider. Services may include: (a) notifications; (b) identity theft protection services; (c) payment of any fines or disallowances imposed by the State or federal government related to the violative collection, use, disclosure, or access; (d) other actions mandated by any law, administrative or judicial order, agency privacy officer, or the Chief Privacy Officer.

ii. At the agency privacy officer's discretion, the Agency may pay for services deemed necessary to address Contractor's collection, disclosure, use, or access of Identifying Information in violation of this Rider. If the Agency pays for any of these services, it may submit invoices to Contractor and Contractor will promptly reimburse the Agency.

iii. Should Contractor refuse to pay for services deemed necessary by the agency privacy officer, then for the purpose of set-off in sufficient sums and without waiver of any other rights and remedies, the City may:

a. withhold further payments under this Agreement to cover the costs of notifications or other actions mandated by any law, administrative or judicial order, or the Chief Privacy Officer, including any related fines or disallowances imposed by the State or federal government; and,

b. withhold further payments to cover the costs of credit monitoring services by a national credit reporting agency and any other commercially reasonable preventive measure.

E. Contractor is not required to make any notification that would compromise public safety, violate any law, or interfere with a law enforcement investigation or other investigative activity by the Agency.

9. Retention.

Contractor will retain Identifying Information as required by law or as otherwise necessary in furtherance of this Agreement, or as otherwise approved by the agency privacy officer.

10. Destruction of Identifying Information.

If the Agency instructs Contractor to destroy Identifying Information, Contractor will destroy it within 30 days after receiving the instruction in a way it cannot be reconstructed, subject to any litigation holds. Contractor will provide written confirmation to the agency privacy officer that it has destroyed the Identifying Information within 30 days after receiving the instruction. If it is impossible for Contractor to destroy the Identifying Information, Contractor will promptly explain in writing why it is impossible, and will, upon receiving the destruction request, immediately stop accessing or using the Identifying Information, and will maintain the Identifying Information in accordance with this Rider.

11. Reporting

Contractor will provide the Agency with reports as requested by the agency privacy officer or Chief Privacy Officer regarding Contractor's collection, use, retention, disclosure of, and access to Identifying Information including: (i) the types of Identifying Information collected, retained, disclosed, or accessed; (ii) the types of collections and disclosures classified as "routine" and any collections or disclosures approved by the agency privacy officer or Chief Privacy Officer; and (iii) any other related information that may be reasonably required by the agency privacy officer or Chief Privacy Officer.

12. Auditing

A. No less than once per year, Contractor shall conduct a comprehensive audit of its privacy program and provide its findings to the Agency.

B. In addition to the auditing required by subsection 12(A), Contractor shall engage a third-party internationally recognized auditor, at Contractor's own cost, to perform periodic audits, scans, and tests, and audit as follows at least once per year and after Contractor collects, discloses, uses, or accesses Identifying Information in violation of this Rider and at the request of the Agency:

    i. a verification of Contractor's compliance with the provisions of this Rider and laws governing Identifying Information;

ii. an assessment of Contractor's privacy practices against recognized industry best practices, and including a gap analysis identifying areas where Contractor's practices fall short of industry best practices and recommending improvements, including assessments of:

a. the necessity the amounts and types of Identifying Information collected;
b. the adequacy of retention and deletion policies;
c. subject rights management;
d. accuracy and understandability of internal and external privacy policies;

C. The Agency may review and audit Contractor's privacy program prior to the commencement of this Agreement and from time to time during the term of this Agreement. Contractor shall allow the Agency to perform audits, and shall fully cooperate and furnish all requested materials in a timely manner. Audits may be conducted by the Agency or an Agency provider and at the Agency's expense. At the Agency's option, Contractor shall complete, within 45 days of receipt, an audit questionnaire provided by the Agency regarding Contractor's privacy program. Contractor shall not be entitled to compensation from the Agency for the time it spends cooperating with any of the audits, scans, or tests provided for in this Section.

13. Coordination with agency privacy officer.

The Agency may assign powers and duties of the agency privacy officer to Contractor for purposes of this Agreement. In such event, Contractor will exercise those powers and duties in accordance with applicable law in relation to this Agreement and will comply with directions of the agency privacy officer and Chief Privacy Officer concerning coordination and reporting.

14. Subcontracts.

A. Contractor will include this Rider in all subcontracts to provide services in connection with this Agreement.

B. Contractor will be responsible to the Agency for compliance with this Rider by its subcontractors in connection with this Agreement.

15. Conflicts with Provisions Governing Records, Reports, and Investigations.

To the extent allowed by law, the provisions of this Rider will control if there is a conflict between any of the provisions of this Rider and, as applicable, Article 5 of Appendix A (General Provisions Governing Contracts for Consultants, Professional, Technical, Human, and Client Services); if Article 5 of Appendix A does not apply, the Investigations Clause, and other provisions concerning records retention and reports designated elsewhere in this Agreement.

16. Construction.

Notwithstanding any contrary provision in this Agreement, to the extent allowed by law, the more restrictive provision concerning collection, use, disclosure of, or access to Identifying Information will control. The provisions of this Rider do not replace or supersede any other obligations or requirements of this Agreement.

Sample Interagency Data Sharing Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

AGENCY C ANALYSIS OF AGENCY A AND AGENCY B DATA

This memorandum of understanding (**MOU**), dated DATE (**Effective Date**), is made between **AGENCY A**, **AGENCY B**, and **AGENCY C** (each a **Party** and collectively the **Parties**) for the purpose of disclosing certain AGENCY A and AGENCY B information to AGENCY C, so that AGENCY C can produce to **AGENCY D** aggregated and summarized data (**Project**).

WHEREAS,; and

WHEREAS,; and

WHEREAS,; and

WHEREAS,; and

WHEREAS,;

NOW, THEREFORE, the Parties agree as follows:

1. **Definitions.**

   a. **Authorized Users** means employees, officials, and agents of AGENCY C whose access to Data is necessary to carry out the Permitted Purpose.

   b. **Data** means the datasets listed in the appendices attached to this MOU (**Appendix A: Data Elements AGENCY A Will Share with AGENCY C and Legal Bases for Sharing; Appendix B: Data Elements AGENCY B Will Share with AGENCY C and Legal Bases for Sharing**).

   c. **De-Identify** means removing identifying information from household-level data for all records included in the Data. Unique Identifiers that an agency may assign to its own Data before transferring it to AGENCY C need not be removed from the Data as long as they cannot be used (other than by the Party creating the Unique Identifier) to identify or locate an individual.

   d. **Identifying Information** means any information that alone or in combination with other information can be used to identify or locate a person.

   e. **Permitted Purpose** means aggregating and summarizing Data to support AGENCY D's purpose.

   f. **Unique Identifier** means a new randomly assigned number a Party creates for each individual whose data it shares with AGENCY C for analysis pursuant to this MOU.

2. **Transfer.** Parties contributing Data will de-identify Data and securely transfer it to AGENCY C via secure file transfer.

3. **Data analysis**. AGENCY C will provide AGENCY D with a summary analysis of and aggregated data.

4. **Legal bases for disclosure**. AGENCY A will disclose its Data to AGENCY C pursuant to the legal bases provided in Appendix A. AGENCY B will disclose its Data to AGENCY C pursuant to the legal bases provided in Appendix B. Any additional Parties will disclose their data to AGENCY C pursuant to legal bases provided in their own respective Appendices.

   Each Party shall independently and separately authorize its own Appendix without need for approval from other Parties.

5. **Confidentiality and data security.**

   a. Except for the Permitted Purpose, AGENCY C will not disclose Data without the respective agency's written permission, subject to 5(h) below.

   b. AGENCY C will not use Data for any purpose except as authorized under this MOU or as required by law.

   c. AGENCY C will limit access to Data to Authorized Users for the Permitted Purpose, and will ensure that Authorized Users understand and comply with the provisions of this MOU applicable to Data.

   d. AGENCY C will not use Data for personal benefit or the benefit of another, nor publish, sell, license, distribute, or otherwise reveal Data.

   e. AGENCY C will use appropriate physical, technological, and procedural safeguards pursuant to the citywide security standards and requirements for data security set forth by the NYC Office of Technology and Innovation and its Office of Cyber Command. All data will be stored on a password-protected, encrypted shared network drive accessible only to Authorized Users.

   f. AGENCY C will treat Data as Restricted Information under the Citywide Cybersecurity Program Policies and Standards issued by the NYC OTI Office of Cyber Command.

   g. If AGENCY C discovers or suspects unauthorized use or disclosure of Data, AGENCY C will promptly:

      i. notify the other Parties, no later than 24 hours after discovery, of:
         1. the discovery of the known or suspected unauthorized use or disclosure;
         2. the date of the use or disclosure;
         3. the name of the user or recipient, if known;
         4. the address of the user or recipient, if known;
         5. the affiliation of the user or recipient, if known;
         6. a brief description of the information used or disclosed;

7. a description of any remedial measures taken to mitigate the effects of such unauthorized use or disclosure of Data, in accordance with all relevant laws;
8. any details necessary for the Parties to know when and how the unauthorized use or disclosure was made;

ii. cooperate with the other Parties and relevant City officials, including the City's Chief Privacy Officer, Office of Cyber Command, and the City's Law Department, to investigate the occurrence and scope of the unauthorized use or disclosure, and make any required or voluntary notices; and

iii. take all reasonably necessary steps to prevent or mitigate damages related to the unauthorized use or disclosure.

h. AGENCY C may disclose Data if required by court order or law. If AGENCY C is required to disclose Data by court order or law, it will:

i. disclose Data only to the extent allowed under a protective order, or

ii. as necessary to comply with the law.

i. Upon termination of the MOU, Agency C shall return all Data in a useable electronic form, and erase, destroy, or render unreadable all Data in its entirety in a manner that prevents its physical reconstruction, and certify in writing that these actions have been completed within 30 calendar days of the termination of the MOU or within seven days of AGENCY B's request, whichever comes first.

6. **Termination and survival.**

a. This MOU commences on the Effective Date and ends on DATE, unless terminated earlier in accordance with this section. The Parties may renew this MOU by mutual written agreement.

b. Any Party may terminate its participation in this MOU for any reason by giving the other Parties 30 days' notice. If this MOU is terminated, each Party will make reasonable efforts to finalize any pending obligations or tasks relating to the terms of this MOU.

c. Section 5 survives the termination, cancellation, or expiration of this MOU, unless the Parties agree otherwise in writing.

7. **Modification.** The Parties can only modify this MOU in writing.

8. **Signing.** This MOU may be executed in counterparts and with electronic signatures.

9. **Additional parties.** Additional agencies may join this MOU by signing an addendum. AGENCY C will notify existing Parties when new Parties are added.

10. **Notices.**

    a. Notices must be in writing and may be sent by email.

    b. Notices must be sent to the following representatives or their designees:

        i. **For AGENCY A:**

        with a copy to:

        ii. **For AGENCY B:**

        with a copy to:

        iii. **For AGENCY C:**

        with a copy to:

    c. Any Party may change its contact information by notice to the other Party. All changes take effect on receipt of notice.

11. **Entire Understanding**

    a. This MOU and attached appendices constitute the entire understanding between the Parties with respect to its subject matter, and is not intended to be a legally binding instrument or create any legally enforceable rights or obligations.

    b. The following document is attached to this MOU:

        i. **Appendix A (Data Elements AGENCY A Will Share with AGENCY C and Legal Bases for Sharing)**

        ii. **Appendix B (Data Elements AGENCY B Will Share with AGENCY C and Legal Bases for Sharing)**

The Parties executed this memorandum of understanding on the dates below their signatures.

NYC

By: _____

Name: _____

Title: _____

Date: _____

NYC

By: _____

Name: _____

Title: _____

Date: _____

NYC

By: _____

Name: _____

Title: _____

Date: _____

Appendix A

Data Elements AGENCY A will Share with AGENCY C and Legal Bases for Sharing

Time period: All data elements to be shared will cover the time period from DATE to DATE, where applicable, to the latest data available as of the Effective Date of the MOU.

Legal Bases for Disclosure:

Data Elements: AGENCY A will share the data elements below from their respective sources with AGENCY C.

Research Goal/Task	Dataset Description	Relevant Timeframe	Row Label (each row describes a...)	Requesting fields that describe (In Parenthesis:)

Appendix B

Data Elements AGENCY B Will Share with AGENCY C and Legal Bases for Sharing

Time period: All data elements to be shared will cover the period from DATE to DATE, where applicable and unless a different period is specified below, to the latest data available as of the Effective Date of the MOU.

Legal Bases for Disclosure:

Data Elements: AGENCY B will share the data elements below, to the extent the data is available from AGENCY B's respective data sources, with AGENCY C.

Research Goal/Task	Dataset Description	Relevant Timeframe	Recency and Fields of Interest (In Parenthesis:)

Sample Interagency Data Integration Scope of Work

Scope of Work Template

Project: Name the project

Project Lead: List the agency that owns the project. It is important to be able to identify the project "owner" because that agency or office leads negotiations and is responsible for managing efforts to achieve the project goals. If you cannot identify which agency is lead for the project, you probably need to refine why the project is happening and how it will work. In some cases there can be more than one project lead.

Additional Partners: List all agencies involved in the project. Sometimes there can be non-agency partners to projects and they may or may not be signatories to the agreement, or you may have subunits of agencies that you want to call out. This space is an opportunity to explain to readers all the different players in the project. If this is a large multi-agency project, it can help to designate agencies as either Data Providers or Data Recipients below. If an agency is neither, do not classify it is either. If it is both, it is acceptable to list it in both places. If those terms do not adequately fit the project, use terms that work better for the project.

> **Data Providers:** List the agencies or entities that will contribute data to the project.
>
> **Data Recipients:** List the agencies or entities will receive data.

Background of Project: Give a narrative description that places the data sharing efforts in context of a larger City or multiagency goal. Questions to consider answering include: Which agency or office has requested the project or initiative and why? What larger City or broad goals will this project support?

Project Goals: Provide a short description of the overall project purpose. What will sharing data achieve?

Details of Data Requested: List the individual names of datasets, spreadsheets, or other data assets that will be shared. For projects with differing levels of data access, specify the data classification for each asset, which staff role or group can have access to the given data asset, and the reason they require access.

If there are only a few field names, or data elements, in each data asset, you may simply list the data elements in this section. If there are many data elements, move this list to a separate data dictionary document, to be attached as an appendix or exhibit.

Project Activities: Describe the project in narrative form. You do not need to be overly formal or technical, but you do want a logical description of each step of the project. Break into subsections if it helps to organize the description. Generally, it is best to describe the project as a series of chronological steps so those reading it can better follow data flow and access. While a narrative description is helpful, supplemental diagrams or other visualizations can greatly clarify and improve understanding, so attach them to the scope of work if appropriate.

Try to be specific about who does what. For instance, instead of saying that an action will occur, say what part/unit of which agency will take the action.

The following guiding questions may help as you try to describe your project's scope. Please note that agency legal counsel must still review and approve the proposed scope before it is included as part of the overall agreement.

1. With which entity or entities does the data originate? Where and to whom does it flow next, and in what format?
    a. Will the City collect any data directly from the public, such as through a public-facing web form? If so, which agency is ultimately collecting and storing the data submitted through the website or other service? Will that agency then share this data with other agencies? What security protocols will the agency use when collecting the public's information?
    b. How are data sets changing over the course of the project? Will new datasets, also called derived datasets, be created as part of the project? "Name" the data using terms consistent with definitions in the overall agreement. Use such labels when describing data flow, access, and restrictions. It will help partners understand the specific data asset described at a given point.
        i. Example: Data contributed by agencies at the project's outset might be "Source Data," and perhaps only certain personnel should have access to it. Once Source Data from different agencies is matched and integrated, it could be labeled "Integrated Data," and descriptions of restrictions may change accordingly. Names and phone numbers extracted from either the Source Data or the Integrated Data and sent to an agency for phone outreach could be labeled "Outreach Data."
2. If this is a multi-agency project, what actions will Data Providers take? Data Recipients? Use these terms to describe actions taken by the entire group.
3. What security protocols will be in place to cover each data transfer? This can also be covered in a separate "Data Transmission Method" section, as noted below.
4. Who needs access to the data at each point? Consider not only staff, but agency contractors approved to collect, use, disclose, or access the information. Note such contractors may need to submit to an Office of Cyber Command application scan.
   Provide further detail about access levels in the "Data Users; Use; Access" section below.

5. At each major juncture, how will the data be used, analyzed, or otherwise worked on? (For example, after initial transfer, will the receiving agency match data? Add its own supplemental data? Perform analytics and create reports?) While specificity is encouraged, do note if project needs require some flexibility in data use so counsel can review. It is useful to leave a comment explaining the need, namely where and why flexibility is required. This will help reduce the need to amend the agreement in the future.
6. Are there any data needs beyond the immediate project scope? For instance, will you need to use any data for project evaluations? Aggregate reporting to leadership? Will an agency need to retain any data for future use?

Data disclosure, use, and access will depend on the restrictions that apply to the data. Your agency counsel will advise you as to whether it is legally possible to perform the project activities as you propose and describe in this section.

Data Users; Use; Access: Describe purpose for which data will be used, specific users to be authorized (by job title and function), and how access will be granted and monitored; include roles and responsibilities chart summarizing partners' obligations if there are complex data access and sharing components to the project.

Data Transmission Method; Data Storage Requirements: Describe how the parties need to store and transmit the data. If project needs demand, name the specific technologies or tools to be used. However, if the project requires some flexibility, use descriptive terminology when outlining the terms rather than identifying specific technologies that may be deprecated before the end of the project. As a practical matter, note that technologies used to handle project data must be approved for such use based on the data's classification type (*see* "Data Classification Standard and Requirements" section).

Data Classification Standard and Requirements: Describe the data as public, confidential, etc., and note any security requirements. If possible, also classify the data using the Citywide Cybersecurity Program Policies and Standards[24] as restricted, sensitive, or non-restricted. While you should leave this section to be determined by agency legal counsel, you can help them by being prepared with information about the source and restrictions on handling the data.

Data Source Matching or Analytics to be Performed: Describe what if any data matching or analytics will be involved and specify by whom it will be provided.

Data ownership and retention: Which agency or agencies will own or retain the data generated by this project when the project is complete? How will it be stored? Will there be any restrictions on access?

[24] *See* NYC Office of Cyber Command Policies, available at: https://cityshare1.nycnet/content/cityshare/pages/cyber-command/cyber-command-policies.

Sample External Non-Disclosure Agreement

NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (**NDA**) is between the City of New York, acting through [agency], located at [agency address], and [vendor], including its current and future affiliates, a [describe Vendor's business], with its primary offices at [vendor's address] (each a **Party** and collectively the **Parties**), in relation to [describe project] (**Project**).

1. The City and [Vendor] agree to collaborate on the Project for the purpose of [Permitted Purpose]. In furtherance of this goal, [Vendor] will [describe Vendor's role]. The Parties may have access to each other's Confidential Information, as such term is defined below, subject to the terms of this NDA.

2. **Definitions**.

    a. **Authorized Users** means employees, officials, and agents of the Receiving Party whose access to Confidential Information is necessary to carry out the Permitted Purpose.

    b. **Confidential Information** means non-public information that the Disclosing Party discloses to the Receiving Party under this NDA, in any form; information derived from non-public information or from information marked as private or confidential; Identifying Information, other than routine business contact information; any other information that a reasonable person knows or should understand to be confidential; and any information that could, if disclosed, reveal the Disclosing Party's proprietary or trade secret information. Confidential Information **does not include** information that is publicly available or known to the Receiving Party prior to its disclosure by the Disclosing Party; is independently developed by the Receiving Party without reference or access to Confidential Information; or is lawfully obtained by the Receiving Party without restrictions on use or disclosure from a third party.

    c. **Disclosing Party** means the Party disclosing its Confidential Information.

    d. **Permitted Purpose** means a use of a Party's information that is necessary to carry out the Party's duties in relation to the Project.

    e. **Identifying Information** means information that alone or in combination with other information may be used to identify or locate an individual.

    f. **Receiving Party** means the Party receiving Confidential Information.

3. **Confidential Information.**

    a. Except in connection with a Permitted Purpose, the Receiving Party will not disclose Confidential Information without the Disclosing Party's written permission, subject to 3(e) below. If [vendor] is the Receiving Party, it will not use Confidential Information in any of its business operations except as needed to process requests or evaluate proposals by [agency], and will not use

Confidential Information for any purpose except as authorized under this NDA or as required by law. The Receiving Party will limit access to Confidential Information to Authorized Users for the Permitted Purpose, and will ensure that Authorized Users understand and comply with the provisions of this agreement applicable to Confidential Information.

b. The Receiving Party will not use Confidential Information for personal benefit or the benefit of another, nor publish, sell, license, distribute, or otherwise reveal Confidential Information.

c. The Receiving Party will use appropriate physical, technological, and procedural safeguards to protect Confidential Information. If the Receiving Party is [agency], these safeguards will conform to the citywide security standards and data security requirements set forth by the New York City Office of Technology and Innovation's Office of Cyber Command. If the Receiving Party is [agency], it will treat Confidential Information as [Restricted or Sensitive] information under the Citywide Cybersecurity Program Policies and Standards. If the Receiving Party is [vendor], it will treat Confidential Information as required by the Cybersecurity Requirements for Vendors and Contractors, available at https://www.nyc.gov/content/oti/pages/vendor-resources/cybersecurity-requirements-for-vendors-contractors.

d. If the Receiving Party knows or suspects unauthorized use or disclosure of Confidential Information, it will promptly

    i. notify the Disclosing Party, no later than seventy-two hours after discovery, of:

        1. the discovery of the known or suspected unauthorized use or disclosure;
        2. the date of the use or disclosure;
        3. the name of the user or recipient, if known;
        4. the address of the user or recipient, if known;
        5. the affiliation of the user or recipient, if known;
        6. a brief description of the information used or disclosed;
        7. a description of any remedial measures taken to mitigate the effects of such unauthorized use or disclosure of Confidential Information, in accordance with all relevant laws;
        8. any details necessary for the Disclosing Party to know when and how the unauthorized use or disclosure was made;

    ii. cooperate with the Disclosing Party and relevant City officials, including the City's Chief Privacy Officer, Office of Cyber Command, and the City's Law Department, to investigate the occurrence and scope of the unauthorized use or disclosure, and make any required or voluntary notices; and

    iii. take all reasonably necessary steps to prevent or mitigate damages related to the unauthorized use or disclosure.

e. The Receiving Party may disclose Confidential Information if required by court order or law. If the Receiving Party is required to disclose Confidential Information by law, it will:

i. promptly notify the Disclosing Party sufficiently in advance of disclosure, but not more than five business days after it learns of the required disclosure, to permit Disclosing Party to seek a protective order and to make any required notifications; and

ii. disclose Confidential Information only to the extent allowed under a protective order or as necessary to comply with the law.

f. If the Disclosing Party instructs the Receiving Party to destroy Confidential Information, the Receiving Party will destroy it no more than five business days after receiving the instruction. The Receiving Party will inform the Disclosing Party that it has destroyed the Confidential Information no more than thirty days after receiving the Disclosing Party's instruction. If it is impossible for the Receiving Party to destroy Confidential Information, the Receiving Party will explain in writing why it is impossible, and will, upon receiving the Disclosing Party's destruction request, immediately stop accessing or using the Confidential Information.

4. **General rights and obligations.**

a. **Law that applies; jurisdiction and venue**. The laws of the State of New York govern this NDA. If federal jurisdiction exists, the federal courts in New York County, New York, have exclusive jurisdiction and venue. If federal jurisdiction does not exist, the Supreme Court in New York County, New York, has exclusive jurisdiction and venue.

b. **Waiver.** If [agency] is the Disclosing Party, its delay or failure to exercise a right or remedy is not a waiver of that, or any other, right or remedy.

c. **Money damages insufficient.** Money damages may be an insufficient remedy for breach or threatened breach of this NDA by the Receiving Party. In addition to all other remedies that the Disclosing Party may have, the Disclosing Party will be entitled to specific performance and injunctive or other equitable relief as a remedy for any breach of the confidentiality and other obligations of this NDA.

d. **Enforceability; severability.** If any part of this NDA is unenforceable, the Parties (or if they cannot agree, a court) will revise it so that it is enforceable. Even if no revision can be enforced, the rest of the NDA will remain in place.

e. **Intellectual property.** This NDA does not give the Receiving Party any intellectual property ownership of or licenses to Confidential Information.

f. **Entire agreement.** This NDA is the entire agreement between the Parties about disclosing Confidential Information in relation to the its subject matter, except that if other contracts between the Parties address Confidential Information, then those obligations remain in force for those contracts.

g. **Modifications.** The Parties can only modify this NDA in writing.

h. **Notices.** Notices must be in writing and may be sent by email. Notices must be sent to the following people or their designees:

   i. **For the City:**

   ii. **For Vendor:**

The Parties are signing this agreement on the dates below their signatures.

City of New York – [agency]

By: _____

Name: _____

Title: _____

Date: _____

Vendor

By: _____

Name: _____

Title: _____

Date: _____

Sample Oversight Data Sharing Agreement

CONFIDENTIALITY AGREEMENT

DISCLOSURE TO OVERSIGHT AGENCY

This confidentiality agreement, dated DATE (**Effective Date**), is made between **AGENCY** and **OVERSIGHT AGENCY** (each a **Party** and collectively the **Parties**) for the purpose of disclosing certain AGENCY information to OVERSIGHT AGENCY.

WHEREAS, APPLICABLE LAW authorizes OVERSIGHT AGENCY to request information from AGENCY; and

WHEREAS, AGENCY'S ability to provide information to OVERSIGHT AGENCY may, in some instances, be restricted by other law's or privileges; and

WHEREAS, New York City's Identifying Information Law, codified at Charter 8 (h) and Administrative Code 23-1201 – 23-1205 requires AGENCY to designate an agency privacy officer, requires the Mayor to designate a Chief Privacy Officer; and requires AGENCY to comply with the Citywide Privacy Protection Policies and Protocols issued by the Chief Privacy Officer; and

WHEREAS, the Identifying Information Law prohibits AGENCY from disclosing any information that may be used on its own or with other information to identify or locate an individual; and

WHEREAS, Citywide Privacy Protection Policies and Protocols 5.2.2.1 requires AGENCY to enter into a confidentiality agreement when a disclosure of identifying information involves a risk of compromising an important privacy interest;

WHEREAS, the Parties want to ensure their compliance with both the law concerning OVERSIGHT AGENCY's authority to secure information and the laws and policies governing AGENCY'S disclosure of identifying information;

NOW, THEREFORE, the Parties agree as follows:

1. **Definitions.**

   a. **Authorized Users** means employees, officials, and agents of OVERSIGHT AGENCY whose access to Sensitive Identifying Information is necessary to carry out the Permitted Purpose.

   b. **Identifying Information** means any information that alone or in combination with other information can be used to identify or locate an individual.

   c. **Sensitive Identifying Information** means Identifying Information that poses a higher risk of harm to an individual or members of an individual's household, by its very nature or under specific

circumstances, and as determined by AGENCY'S agency privacy officer or by the Chief Privacy Officer.

d. **Permitted Purpose** means carrying out OVERSIGHT AGENCY'S mission or purpose.

2. **Applicability.**

a. This agreement covers Sensitive Identifying Information responsive to OVERSIGHT AGENCY'S request, where AGENCY'S agency privacy officer or the Chief Privacy Officer have determined that the Identifying Information Law requires a confidentiality agreement.

b. The Sensitive Identifying Information covered by this agreement is described in **Attachment A**.

3. **Legal bases for disclosure**.

a. OVERSIGHT AGENCY'S LEGAL BASIS TO COMPEL AGENCY TO PRODUCE INFORMATION.

b. Except for information as to which AGENCY is asserting a privilege or other legal basis for nondisclosure, either AGENCY'S agency privacy officer or the Chief Privacy Officer have approved disclosing Sensitive Identifying Information to OVERSIGHT AGENCY.

4. **Confidentiality and data security.**

a. OVERSIGHT AGENCY will limit access to Sensitive Identifying Information to Authorized Users for the Permitted Purpose.

b. OVERSIGHT AGENCY will ensure that Authorized Users understand and comply with the provisions of this agreement applicable to Sensitive Identifying Information.

c. OVERSIGHT AGENCY will use appropriate physical, technological, and procedural safeguards at least as protective as the Citywide Cybersecurity Program Policies and Standards set forth by the NYC Office of Technology and Innovation through its Office of Cyber Command.

d. If OVERSIGHT AGENCY is an agency of the City of New York, it will treat Sensitive Identifying Information as Restricted information under the Citywide Cybersecurity Program Policies and Standards.

e. OVERSIGHT AGENCY will anonymize Sensitive Identifying Information in published reports and will delete or redact information in published reports that could identify or locate individuals associated with Sensitive Identifying Information, unless AGENCY agrees otherwise in writing or including Sensitive Identifying Information is required by law.

f. The Parties will follow this procedure if OVERSIGHT AGENCY receives a third-party request for Sensitive Identifying Information:

i. OVERSIGHT AGENCY will promptly notify AGENCY of the request and will provide a copy of the request to AGENCY, unless following this procedure is prohibited by law.

ii. OVERSIGHT AGENCY will propose a response to the request to AGENCY, considering the laws governing Sensitive Identifying Information, at least fourteen days before responding to the request.

iii. AGENCY will respond to OVERSIGHT AGENCY within 7 days of receiving the proposed response to indicate whether AGENCY believes the proposed response adequately protects Sensitive Identifying Information.

iv. OVERSIGHT AGENCY and AGENCY will confer in good faith to resolve any disputes.

v. If AGENCY intends to seek a protective order, it will notify OVERSIGHT AGENCY within at least 7 days before so seeking. OVERSIGHT AGENCY will not disclose Sensitive Identifying Information until AGENCY'S action is resolved or after 14 days' notice to AGENCY is no action is initiated.

g. If OVERSIGHT AGENCY discovers or suspects unauthorized use or disclosure of Sensitive Identifying Information, OVERSIGHT AGENCY will promptly:

i. notify AGENCY, no later than 24 hours after discovery, of:
   1. the discovery of the known or suspected unauthorized use or disclosure;
   2. the date of the use or disclosure;
   3. the name of the user or recipient, if known;
   4. the address of the user or recipient, if known;
   5. the affiliation of the user or recipient, if known;
   6. a brief description of the information used or disclosed;
   7. a description of any remedial measures taken to mitigate the effects of such unauthorized use or disclosure of Sensitive Identifying Information, in accordance with all relevant laws;
   8. any details necessary for the Parties to know when and how the unauthorized use or disclosure was made;

ii. cooperate with the other Parties and relevant City officials, including the City's Chief Privacy Officer, Office of Cyber Command, and the City's Law Department, to investigate the occurrence and scope of the unauthorized use or disclosure, and make any required or voluntary notices; and

iii. take all reasonably necessary steps to prevent or mitigate damages related to the unauthorized use or disclosure.

h. OVERSIGHT AGENCY will destroy Sensitive Identifying Information that is no longer required to support the Permitted Purpose, to the extent that destroying Sensitive Identifying Information is consistent with OVERSIGHT AGENCY'S records retention rules and applicable law.

5. **Signing.** This MOU may be executed in counterparts and with electronic signatures.

6. **Notices.**

   a. Notices must be in writing and may be sent by email.

   b. Notices must be sent to the following representatives or their designees:

      i. **For AGENCY:**

      with a copy to:

      ii. **For OVERSIGHT AGENCY:**

      with a copy to:

   c. Either Party may change its contact information by notice to the other Party. All changes take effect on receipt of notice.

7. **Entire Agreement**

   a. This agreement and attached appendices constitute the entire agreement between the Parties with respect to its subject matter. This Agreement supersedes all previous or contemporaneous oral or written agreements between the Parties with respect to its subject matter.

   b. The following document is attached to this agreement:

      i. **Attachment A** (Sensitive Identifying Information disclosed by AGENCY to OVERSIGHT AGENCY

[Remainder of page intentionally left blank.]

The Parties executed this agreement on the dates below their signatures.

AGENCY

By: _____

Name: _____

Title: _____

Date: _____

OVERSIGHT AGENCY

By: _____

Name: _____

Title: _____

Date: _____

Employee or Volunteer Simple Non-Disclosure Agreement

EMPLOYEE CONFIDENTIALITY/NON-DISCLOSURE AGREEMENT

Name and Address of Employee (**Employee**):

_____

_____

_____

This Confidentiality/Non-Disclosure Agreement is between the [Agency] and Employee. Employee states:
I am assisting the [Agency] in working on [project] concerning available City and other resources and services (**Project**);

During the course of work on the Project, I may receive personal information from the [Agency] that is confidential, including the names, addresses, phone numbers, and other personal contact information of individuals (**Confidential Information**);

I will protect Confidential Information by storing it securely and not disclosing it to any unauthorized party unless I have been authorized in advance, and in writing, by the [Agency];

I will not use Confidential Information except for purposes related to the Project, and I will not access, use, sell, or otherwise disclose Confidential Information to anyone not participating in the Project, unless authorized by the [Agency] or as required by law;

Where I am authorized by the [Agency] to collect or store Confidential Information, I will maintain such information only on City-provided devices or, with prior written permission from the [Agency], on devices that I own;

I will immediately notify the [Agency] if I lose or misplace Confidential Information, or if I suspect or know that an unauthorized party accesses or uses the Confidential Information;

I will immediately destroy Confidential Information in my possession when asked by the [Agency], or if not requested, at the end of my assignment to the Project;

I will follow all relevant laws and City policies for protecting the privacy and security of Confidential Information; and

I will immediately ask the [Agency] for help if I have questions about handling Confidential Information.

Print Employee Name: _____

Employee Signature: _____ Date: _____

Agency Signature/Title: _____ Date: _____