PPB: MyPDConnect

Privacy Impact and Risk Analysis

Final draft

Smart City PDX

June 30, 2025

PRIVACY ANALYSIS REPORT

City of Portland Privacy Toolkit

WHAT IS PRIVACY RISK AND IMPACT ANALYSIS?

The Privacy Impact Analysis ("PIA") is a method to quickly evaluate what are the general privacy risks of a technological solution or a specific use, transfer, or collection of data to City bureaus or offices. The PIA is a way to identify factors that contribute to privacy risks and lead to proper strategies for risk mitigation or alternatives that may even remove those identified risks.

The Privacy Impact Analysis may lead to a more comprehensive Impact Assessment and a Surveillance Assessment depending on the level or risks identified and the impacts on civil liberties or potential harm in communities.

In the interests of transparency in data collection and management, the City of Portland has committed to publishing all Privacy Assessments on an outward facing website for public access. PIAs do not include specific uses of technology or data other than those initially evaluated.

WHEN IS PRIVACY IMPACT ANALYSIS RECOMMENDED?

A PIA is recommended when:

- A project includes surveillance technologies.
- A project, technology, data sharing agreement, or other review has been flagged as having some privacy risk due to the collection of private or sensitive data.
- A technology has high financial impact and includes the collection, use or transfer of data by city bureaus or third parties working for or on behalf of the city.

WHAT IS IT INCLUDED IN A PRIVACY IMPACT ASSESSMENT?

City staff completes two sections included in a privacy impact assessment report:

- *The Privacy Analysis form.* This document identifies all important information related to the project description, data collection, use, safekeeping, and management; as well as a verification of existing privacy policies and measures to protect private information.
- *The Privacy Risk Assessment.* This document breaks the privacy risk into six different areas of evaluation: (I) Individual Privacy Harms; (II) Equity, Disparate Community Impact; (III) Political, Reputation & Image; (IV) City Business, Quality & Infrastructure; (V) Legal & Regulatory; and, (VI) Financial Impact. Then compares risks to the likelihood of creating a single risk measure based on the worst-case scenario.

Executive summary

The Portland Police Bureau is looking to replace its current online incident report application, CopLogic, with a solution from MyPDConnect. Online reporting provides a convenient way to report crimes that do not involve an active threat or emergent crisis. Information submitted via this website can also be used as evidence in a criminal case.

The information submitted in an incident report includes personal and demographic information. This service enables community members to describe the incident and upload documents, pictures, and video to support the narrative, which may also include sensitive information. All the information shared in the incident report can be considered as evidence in a criminal case and will be managed with high security protections.

The Portland Police Bureau uses the data generated from these reports to identify patterns and trends across the city. This helps PPB to develop new strategies for addressing crime and distribute agency resources to the areas of greatest need.

No major risks have been identified, and the worst-case scenario is set with a *Medium Risk* level.

The table below describes the main risks identified in this assessment.

Risk area	Risk level	Highlighted risks
Individual Privacy Harms	Medium	The risk of collecting sensitive information unnecessarily and then publicly releasing it is the highest risk identified in this project. The recommendation is to minimize the collection of unnecessary information for the purpose of this forms, which is incident reporting. Additional demographics information can be collected in a separate and optional form that is not linked to the original name or personal address.
Equity, Disparate Community Impact	Medium	The highest equity risk is the unintentional use of sensitive information for identifying specific groups. This segregation of individuals by demographics can be used for other purposes by third parties.
Political, Reputation & Image	Medium	Risks derived from public trust issues are included in this section. Mistrust from specific demographic groups may reduce the chances that individuals from these groups share information or report incidents to Police. The idea of potential use of personal information for other purposes, like sharing that with agencies like ICE or other Federal agencies, may impact on the likelihood that someone shares

Risk area	Risk level	Highlighted risks
		sensitive information in this form.
City Business, Quality & Infrastructure	Medium	The only issue identified is the risk of unauthorized access to restricted information. Portland Police is already implementing the highest standards on cybersecurity and information management in the City of Portland and the likelihood of this risk is very low. However, if it happens, impacts can be high due to a detriment in trusting existing information security measures.
Legal & Regulatory	Medium	Risk of Civil Rights complaint under Title VI. If a translation is inaccurate, there can be the risk of a community member filing a formal civil rights complaint under Title VI. Inaccuracy in information on a report of this nature can have significant consequences for people involved and can result in a formal civil rights complaint to the police bureau and city.
Financial Impact	Low	Financial risks are low due to the scope of this project. There is a possibility of receiving compensation claims due to damage created by privacy breaches. Given that privacy breaches are unlikely, the risk is low.

Privacy Analysis

Purpose of the technology, project, data sharing or application

Portland Police Bureau currently offers a **non-emergency** issue reporting site that is planned to have a platform called *MyPDConnect*[1].

Online reporting provides a convenient way to report crimes that do not involve an active threat or emergent crisis. When people use the online system, it saves time to the police by focusing on existing resources.

The collection of information includes personal identifiable information, description of the crime being reported, and additional content to support the report. Information collected by Portland Police via the incident reporting site can be used as evidence in a criminal case.

The Portland Police Bureau uses the data generated from these reports to identify patterns and trends across the city. This helps PPB to develop new strategies for addressing crime and distribute agency resources to the areas of greatest need.

The Portland Police Report online submission page is https://www.portland.gov/police/cor

MyPDConnect is the tool selected to replace the existing backend data collection system. MyPDConnect defines itself as providing a "Next Generation Online Reporting and Virtual Policing Solution".

It offers features like mobile-first crime reporting, diverting calls from dispatch centers to online reporting, and virtual meetings with officers. And, it allows users to upload pictures, videos, and documents directly to an agency's Axon Evidence repository. MyPDConnect has been certified as a third-party vendor by Axon. There is no manual transferring of information from MyPDConnect to other systems, especially any system other than Portland Police’s Records Management System (RMS) and Evidence.com.

Name of the entity owner of the application and website

MyPDConnect
https://www.mypdconnect.com/index.html

Type of Organization

Private Entity

[1] https://www.mypdconnect.com/

Scope of personal data collected. List all sources of data and information.

Individuals will report criminal issues through the Portland Police Bureau report online site.

The current personal data collected by this reporting site includes:

- Name
- Home Address
- Work address (optional)
- Home phone (optional)
- Mobile phone (optional)
- email address
- employer name (optional)
- work phone (optional)
- Race
- Date of Birth
- Sex
- Resident status (resident, not resident)

Personal information requested when applicable:

- ID number(s) when ID is stolen

Race, age, and sex are required fields by the National Incident-Based Reporting System (NIBRS)[2]. Age is derived from date of birth

Date of Birth is a required field to comply with the Standard Functional Specifications for Law Enforcement Records Management Systems (RMS)[3].

The 'Resident status' field will be described with a Boolean field answering the question: "Do you live in the City of Portland?". This change will clarify the purpose of this information to match the NIBRS requirements.

Individuals can also submit documents, pictures, or videos. These media documents may also include personal and sensitive information that may need to be redacted when publicly disclosed.

How personal data is collected.

Personal data is collected through the website. For incident reporting, no additional information is added.

[2] https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/ucr/nibrs

[3] https://ijis.org/community-resources/standard-functional-specifications-for-law-enforcement-records-management-systems/

Who can access the data?

Authorized PPB personnel. Records are available via public records requests.

Purposes the data is used for.

The Portland Police Bureau uses the data generated from these reports to identify patterns and trends across the city. This helps PPB to develop new strategies for addressing crime and distribute agency resources to the areas of greatest need.

Information submitted via the website can also be used as evidence in a criminal case.

This data will also be used by the Portland Police Bureau's work, including investigatory follow-up, data analysis, NIBRS (National Incident-Based Reporting System)[4] reporting, and evidence for prosecution.

Online reports are imported into RegJIN[5] (Regional Justice Information Network) and they are treated like reports written by officers. Any online report for a Group A crime[6] would be included in the Group A Crime open data. The reports are not specifically identified as online reports. The data does not contain any information related to the people making the reports or involved in the incident. Address information is only provided at the 100-block level. Open data information does not include sensitive information.

Where the data is stored

Data is stored on vendor's servers, then sent to Portland Police Bureau's server.

MyPDConnect will integrate with Axon's Evidence.com. MyPDConnect has been certified as a third-party vendor by Axon. There will not be any manual transferring of information from MyPDConnect to other systems, especially any system other than PPB's Records Management System and Evidence.com.

How data is shared

Query only access by law enforcement agencies via authorized users.

Data is shared during discovery to the District Attorney's Office, and it's shared during public records requests via GovQA.

[4] https://www2.fbi.gov/ucr/faqs.htm
[5] https://www.portland.gov/police/divisions/regjin
[6] https://www.portland.gov/police/open-data/crime-definitions

How long is the data stored?

Data is stored until retention period ends. Retention times vary depending on whether a report is part of an ongoing investigation or the type of crime. Current retention schedules can be downloaded in this page: https://www.portland.gov/auditor/archives/retention-schedules.

Retention time varies depending on whether a reporting is part of an ongoing investigation and the type of crime:

LE-0170 Incident Case Records - a) Homicides and dead body records, retain permanently; (b) Measure 11 and sex crimes, retain 60 years; (c) Explosives-related, retain 30 years; (d) All other cases, retain 20 years.

LE-0270 Evidence/Property Records - (a) Homicide, retain Permanent; (b) Measure 11 and sex crimes, retain 60 years; (c) Cases involving crimes with no statute of limitations, retain 75 years after case closed; (d) all other cases retain 10 years after last action.

Effectiveness

The product is an information collection system that includes sensitive and personal information. This product complies with the Criminal Justice Information System (CJIS) cybersecurity standards, and it is deployed in the Microsoft Azure Government Cloud. This ensures fulfilment of the City's cybersecurity compliance.

The collection of sensitive personal data like sex, date of birth, and personal address may deter some individuals from reporting crimes.

Submitters of an incident can correct or add more information to a specific report.

The UX design and accessibility limitations could be a factor in how victims interact with the website.

Necessity & Proportionality, fundamental rights, frequency of the collection, and data protection and privacy issues line unintended data collection or processing.

Necessity and proportionality. Some sensitive information may be required to describe a crime properly. Reporting criminal events is a heavily emotional task, and details may help investigations and the justice system to be as effective as it can be.

These intake forms specify what fields are mandatory and what can be left empty or are optional. Some mandatory fields in the current intake form can create privacy risks due to the level of sensitivity; however, mandatory fields are necessary to comply with existing State and Federal crime incident reporting systems.

This reporting tool allows submitters to update the form and edit or add details to it after submission.

Since this information is directly collected by Portland Police Bureau, these fields are not protected by the Criminal Justice Information System privacy safeguards. Public records request on these submissions may make this information available to the public.

Privacy safeguards

Information is stored in Portland Police Bureau servers and processed by authorized users for specific purposes.

Portland's Instance of MyPDConnect would only let access to authorized users. In addition, MyPDConnect offers Azure/Entra ID SSO, which is what Portland will be using on the release version.

Portland Police Bureau records management staff do redact information in public records requests; they also blur images containing sensitive or personal information in them, including people's faces.

Open source

No

AI/ML claims

No

Privacy Policy (link)

https://www.mypdconnect.com/privacypolicy.html

Privacy risk

Medium. Some risks need to be mitigated.

Surveillance Tech?

No

Portland Privacy Principles (P3)

Data Utility

The collection of information via Portland Police Bureau's reporting site brings great value to ongoing investigations, law enforcement strategies, and general crime prevention planning.

Some personal information is required to validate the submission and follow up. However, some demographic information aiming to measure equity metrics is not necessary for the purpose of the collection of the information.

Full lifecycle stewardship

Portland Police Bureau staff keep full lifecycle stewardship from collection to destruction of the information following existing retention schedules. The Portland Police Records team serve public records requests and keep exempt and private information redacted or blurred.

Transparency and accountability

Submitters using this reporting form can add or follow up from a submitted report by using the unique number assigned to each report.

Portland Police keeps an active open data dashboard with information about criminal incidents in the city: https://www.portland.gov/police/open-data

Ethical and non-discriminatory use of data

These forms are publicly available and the use of the new MyPDConnect platform will allow users to easily create translated versions of the form.

Demographic information is collected with submission. This creates some risks for the submitter but also enables equity analysis and potentially more culturally appropriate follow-ups. This creates some ethical conflicts and the potential to mitigate some of these issues with the new platform.

Data openness

The Portland Police Bureau has an open data program that proactively releases aggregated and anonymized information about Police activity in Portland.

https://www.portland.gov/police/open-data

Automated Decision Systems

No automated decisions include this information.

Consent.

The Police reporting site is an active action that people take to report crime incidents. They opt-in when they submit a new case or form.

Privacy Impact Risk Severity Assessment

WORST CASE SCENARIO	MEDIUM

Baseline (B): (T) – Technology level, (U) – use and application level.

Risk type (RT): (I) Individual Privacy Harms; (II) Equity, Disparate Community Impact; (III) Political, Reputation & Image; (IV) City Business, Quality & Infrastructure; (V) Legal & Regulatory; and (VI) Financial Impact.

B	RT	ID	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
U	I	1	Individual Privacy Harms				
T	I	1.1	Risk of a privacy breach	High	unlikely	This is a generic privacy risk derived from the collection of private or sensitive information. In this case, MyPDConnect will collect the submitter's personal information. Privacy breach is the unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that an entity maintains.[7] Portland Police data management follows the strictest cybersecurity practices in the City of Portland due to type of operations and sensitive information that is regularly processed. All data breaches need to be reported to the State of Oregon	Medium
U	I	1.2	Risk of collecting sensitive information unnecessarily	Moderate	unlikely	The collection of demographic information is not necessary for reporting a criminal issue or concern by an individual; however, some personal information still is necessary, including information that validates the identity of the submitter. This includes race, sex, date of birth, and Portland Police district residency status. The City of Portland's Privacy and information principle of data utility recommends only collecting the minimum amount	Low

[7] https://www.oregonlegislature.gov/bills_laws/ors/ors646A.html

B	RT	ID	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
						of personal information for a defined purpose that brings value to the community and the City. Adding more personal description to an individual profile creates more privacy risks, particularly when this information can be publicly released or shared. Collecting addition of demographic information can support to reach the City's equity goals and offer better customer service. The recommendation is to create secondary surveys that unlink demographic information from a specific profile and still collect information needed to track or comply with equity goals at the City. If unlinking additional personal information is not possible, then define these fields as optional and inform submitters that this information can be publicly disclosed.	
U	I	1.3	Risk of releasing sensitive information via a public records request.	High	Possible	The information collected by the incident reporting site includes identified sensitive information including race, date of birth, and sex. Also, the submitter can include additional sensitive information in the form of documents, images, or videos. District Attorney's past decisions require the City of Portland to release information that is not explicitly exempt from public records requests[8][9][10]. This information includes information collected using the incident reporting form. Mitigating this risk can include separation of the collection of sensitive information if this is not needed and informing the submitter, potentially with an explicit consent window, about the potential public release of the information shared with the City.	Medium

[8] Date of birth.https://www.mcda.us/wp-content/files_mf/13516496840905.pdf and https://www.mcda.us/wp-content/files_mf/13516496960906.pdf
[9] Names of members of the public. https://www.mcda.us/wp-content/files_mf/15154573231763Order.pdf
[10] Names of officers involved in shooting. https://www.mcda.us/wp-content/files_mf/13516431791006.pdf

B	RT	ID	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
T	I	1.4	Risk of identity theft derived from public release of personal information.	High	unlikely	Public release of personal identifiable information can increase the risk of identity theft. Linked information like personal name, address, and date of birth can multiple the possibilities of identity theft[11]. Minimizing the personal information collected by the incident reporting site can reduce the risk of potential identity theft. Collect just the required information for an investigation.	Medium
T	II	2	Equity, Disparate Community Impact				
U	II	2.1	Risk of using sensitive information for identifying specific groups for other purpose.	Moderate	Possible	Sex, race and ethnicity are sensitive information that can be used to target specific groups. This information is necessary to comply with State and Federal crime incident reporting data standards. Portland Police can build procedures that ensure that this information will be only used for incident reporting and follow existing laws and regulations attached to a criminal case. The recommendation is only collecting the necessary information required to comply with regulations and data standards.	Medium
U	II	2.2	Risk of underrepresentation of specific groups due to misleading demographic data collection.	Moderate	unlikely	Some people may not share demographic data due to fears of sharing this information with the Police. This may create unknown bias about people submitting criminal incidents. Clearly informing how the information is used, protected, shared or released, and eventually destroyed can improve public trust and enable sharing personal information. Creating an open data dashboard informing how incidents reporting site and data are used and effectiveness of the reporting can also improve public confidence. Also, adding privacy and information protection notices can improve public trust.	Low

[11] https://www.usa.gov/identity-theft

B	RT	ID	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
T	II	2.3	Risk of missing privacy protections in non-English submissions.	High	Possible	Submitters can choose to translate the form into another language using the google translate integrated app. When the report is submitted, it is re-translated into English. A copy of the original report (in the foreign language) is kept. Given the importance and impacts of this crime incident reporting tool, Portland Police should use the meaningful access statement paired with the multilingual "add-on". Information about meaningful access statements can be accessed in this page: https://www.portland.gov/officeofequity/equity-title-vi-division/civil-rights-and-meaningful-access-statements Regarding automated translations systems, the likelihood of accurate translations is better in more popular languages, while others may have translation errors or misrepresent the original sentence. The person reporting a crime has the civil right to make the report with a professional interpreter or translator if requested. Any machine that has translated information related to crime and used in a judicial process needs to have a professional, human translator review to ensure accuracy[12]. Inaccuracy in information on a report of this nature can have significant consequences for people involved and can result in a formal civil rights complaint to the police bureau and city. All machine translation must have a human review. All members of the community filing these reports in their language of preference have the right to accurate, equitable and meaningful engagement and communication same as any English fluent community member (in accordance with Civil Rights Law and City Policy).	Medium

[12] Title VI of the Civil Rights Act of 1964, City of Portland Language Access Policy. https://www.portland.gov/officeofequity/language-access

B	RT	ID	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
						There is high risk of inaccuracy and thus inaccurate reporting and consequential judicial issues if these reports are filed in other languages using only machine translation. Recognizing that some languages may need additional resources and support to verify facts and crime reports, particularly in a potentially highly emotional context. It is the individual's civil right to request language assistance in their language of preference, at no cost to them to place the report. Portland Police can offer to get them an interpreter or translator, or the member of the public can request one. High stakes incidents may need an expert translator to verify accuracy of the final English translated submission.	
T	III	3	Political, Reputation & Image				
U	III	3.1	Risk of mistrust from specific demographic groups.	Moderate	Possible	Some people may not share criminal incidents due to the collection of this information about them. There is mistrust when the City collects and manages personal information without informing the public how this information will be used and protected. Transparency on how incident reporting information is used can improve people’s trust in general. Public information on the benefits of incident reporting, highlighting information protection measures and effectiveness of reporting can offer metrics that incentivize public participation. It might be needed to explore deeper on how this risk impacts specific groups or neighborhoods.	Medium
U	III	3.2	Risk of using this information for other purposes.	Moderate	Possible	Information collected via the incident reporting site will support Portland Police focus resources and find trends for better planning. Some reporting entries can be used as evidence in criminal investigations. Purposes outside the initial use of this information may impact public trust and increase privacy risks like breaches and re-identification of already anonymized or obfuscated data. Further analysis may be needed to identify other uses	Medium

B	RT	ID	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
						of information and downstream the data pipeline and it is part of other information systems.	
T	IV	4	City Business, Quality & Infrastructure				
T	IV	4.1	Risk of unauthorized access to restricted information	High	unlikely	Unauthorized access to the information collected via the incident reporting site can be derived from privacy data breaches or other privacy risks. Unauthorized access can come from different sources, and they can be intentional or unintentional. Post event analysis must be done when authorized access is detected. Constant monitoring of data access logs and secure integration into other information systems are strategies that can reduce impacts of this risk. Portland Police already is implementing cybersecurity best practices in compliance with the City of Portland's policies and administrative rules. Also, the Bureau of Planning and Sustainability's Information Security group supports and assesses cybersecurity risks.	Medium
U	V	5	Legal & Regulatory				
U	V	5.1	Risk of legal action against the City due to privacy breaches.	Moderate	unlikely	There is a risk of lawsuits against the City claiming damages derived of any data privacy breach. Reducing this risk implies minimizing the collection of personal identifiable information to the required data, anonymizing or aggregating information in publicly available data, and keeping good data management hygiene will reduce the likelihood of this risk.	Low
U	V	5.2	Risk of Civil Rights complaint under Title VI.	High	Possible	If an automatic translation is inaccurate and results in personal harm or economic losses, there can be the risk of a community member filing a formal civil rights complaint under Title VI.	Medium

B	RT	ID	Risk description	Impact	Likelihood	Mitigation, comments, and strategies	Risk level
						A Title VI complaint in Oregon is a formal way to report discrimination based on race, color, or national origin in programs or activities. Portland Police can ensure following the City's policy[13] and recommendations to add meaningful access statements as baseline to the services offered online. The effectiveness of translations is in direct connection with how the incident is managed. PPB needs to demonstrate that all reasonable efforts are implemented to assure effective translations when an incident is reported in languages other than English.	
T	VI	6	Financial Impact				
T	VI	6.1	Risk of unplanned compensation claims due to damage created by privacy breaches or other legal risks.	Moderate	unlikely	Damage compensation claims can be unplanned expenses, and they can also reduce public trust in information management systems. Reducing this risk is connected to the reduction of data breaches and the effective implementation of information securing practices.	Low

[13] https://efiles.portlandoregon.gov/recordhtml/14037336/

Appendix A
Privacy risk assessment framework

Severity (Evaluate for the worst / highest possible impact)				
	A: Low	**B: Moderate**	**C: High**	**D: Extreme**
Individual Privacy Harms	Customer or “telephone book” information collected and could be disclosed (excluding utility customer data, protected by RCW)	Potential disclosure would be limited to non-financial, non-health related information; no personal identifiers (e.g., social security and driver’s license #s)	Financial or other highly sensitive information would be collected and disclosable requiring action to remediate negative effects (example: non-HIPAA health data); i.e., credit report management required	Disclosure would result in extreme privacy impacts on highly regulated information; catastrophic public release of financial and personal information requiring credit report monitoring and other remediation
Equity, Disparate Community Impact	Little or no equity impact, technology delivered uniformly without reference to individuals or demographic groups	Accidental or perceived disparate impact to communities by nature of location of technology or service delivered	Intentional disparate equity impact resulting in community concern resulting in privacy harms, media coverage; loss of reputation, legitimacy and trust impacted	Extreme impacts to community, City experiences national media attention; widespread public concern and protest; significant breakdown in business processes associated with damage control
Political, Reputation & Image	Issues could be resolved internally by day-to-day processes; little or no outside stakeholder interest.	Issues could be raised by media and activist community resulting in protests and direct community complaints	Disclosure would likely result in heavy local media coverage; reputation, legitimacy and trust impacted	Likely national and international media coverage; serious public outcry; significant breakdown in business processes associated with mitigation and damage control

City Business, Quality & Infrastructure	Management of disclosure issues would represent negligible business interruption; resolved with no loss of productivity	Issue management would result in brief loss of services; loss of < 1 week service delivery; limited loss of productivity	Significant event; loss of > 1–3-week loss of services; critical service interruption to delivery of infrastructure services	Extreme event; business collapse for department services; loss of > = 3 months of data or productivity; critical business infrastructure loss > 1 month
Legal & Regulatory	Adverse regulatory or legal action not indicated or highly unlikely	Relatively minor incident, regulatory action unlikely; possible legal intervention or consultation for addressing data exposure or loss	Adverse regulatory action likely – i.e., fines and actions associated with CJIS, HIPAA, PCI, NERC, COPPA violations, etc.	Major legislative or regulatory breach; investigation, fines, and prosecution likely; class action or other legal action
Financial Impact	$0-$500 impact; internal costs covered, and no significant external costs incurred	>$500 - $5,000; internal and external costs associated with legal consultation, system rework, overtime	> $5,000 -$50,000 external costs associated with fines, consultation fees and regulatory actions to mitigate information exposure; internal costs associated with system rework, overtime	> $50,000 external costs associated with fines, consultation fees and regulatory actions to mitigate information exposure; internal costs associated with system rework, overtime

Likelihood analysis.

For assessing probability of risks

Likelihood	Probability
Almost certain	Likely to occur yearly
Likely	Likely to occur every 2 years
Possible	Likely to occur every 5 years
Unlikely	Likely to occur every 10-20 years
Rare	Has never occurred

Risk Matrix

	Low	Moderate	High	Extreme
Almost Certain	🟧	🟧	🟥	High
Likely	🟩	🟧	🟥	🟥
Possible	🟩	Medium	🟧	🟥
Unlikely	🟩	🟩	🟧	🟥
Rare	Low	🟩	🟧	🟧

Appendix B
Definitions

Automated Decision System	A process, set of rules, or tool based on automated processing of data to perform calculations, create new data, or to undertake complex reasoning tasks. This includes advanced methods like artificial intelligence and machine learning, visual perception, speech or facial recognition, and automated translation between languages.
Data	Statistical, factual, quantitative, or qualitative information, in digital or analog form, that is regularly maintained or created by or on behalf of a City bureau and is in a form that can be transmitted or processed.
Data Governance	Definition of policies, processes and framework of accountability to appropriately manage data as a strategic asset.
Digital Age	This current era whereby social, economic and political activities are dependent on information and communication technologies. It is also known as the Information Age or the Digital Era.
Information	Information is the result of Data being processed, organized, structured or presented, allowing it to be used and understood.
Information Protection	A system of Data processing practices related to personally identifiable or identifying Data for the protection of privacy. This includes the management of individual pieces of personal Information, securing Data against unauthorized access, corruption or loss.
Metadata	A set of Data that describes and gives information about other Data, including its description, origination, and accuracy.
Open Data	Data that can be freely accessed, used, reused and redistributed by anyone.
Personal Information	Information about a natural person that is readily identifiable to that specific individual. “personal information,” which include, but are not limited to: • identifiers such as a real name, alias, postal address, unique personal identifier, online identifier IP address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers; • payment card industry such as bank account numbers or access codes; • personal health data, such as health history, symptoms of a disease, current health care information, medical device identifiers and serial numbers; • commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;

	• biometric information; • internet or other electronic network activity information, that includes browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement; • geolocation data, vehicle identifiers (including serial numbers and license plate numbers); • audio, electronic, visual, thermal, olfactory, or similar information; • professional or employment related information; • education information, provided that it is not publicly available; and • inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes
HRAR 11.04 Protection of Restricted and Confidential Information	
Privacy	The ability of an individual to be left alone, out of public view, and in control of information about oneself.
Confidential	Information that is made confidential or privileged by law or the disclosure of information that is otherwise prohibited by law or City policy.
Restricted	Some restrictions or limitations on the use of or disclosure of the information.
Principle of proportionality	The principle of proportionality requires that the processing of personal information must be relevant to, and must not exceed, the declared purpose
Surveillance Technologies	technologies that observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice.
Privacy terms	
Effectiveness	This refers to how a specific technology or solution fulfills the pursued objective.
Proportionality	Proportionality is a privacy principle that personal data collected and processed should be adequate, relevant, and limited to that necessary for purpose processed. Proportionality has multiple dimensions. Data collected and used should be adequate, because collecting too little information may lead to incorrect or incomplete information on a data subject. It should also be relevant and limited to what is necessary in relation to the purposes for which it is collected and processed (data minimization’), both in terms of scope and time (data

	retention). The proportionality principles consideration of the amount of data to be collected. If excessive data is collected in relation to purposes, then it is disproportionate. Examples: Using biometric data like fingerprints to identify individuals when ID cards suffice.
data protection	Data protection is the process of protecting data and involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes. Data protection is also known as data privacy or information privacy. Data protection should always be applied to all forms of data, whether it be personal or enterprise. It deals with both the integrity of the data, protection from corruption or errors, and privacy of data, it being accessible to only those that have access privilege to it.
Frequency of the collection	Periodicity of the data collection.
Privacy safeguards	Measures designed to improve privacy and information protection. It can be represented as below, as, or greater than industry standard and best practices
privacy fundamental rights	Privacy fundamental rights are set to help individuals in being assured of the protection and privacy of their personal data. The General Data Protection Regulation contains a set of 8 privacy fundamental rights. These rights are not legally binding in the US.
Right to information	This right provides the individual with the ability to ask for information about what personal data is being processed and the rationale for such processing. For example, a customer may ask for the list of processors with whom personal data is shared.
Right to access	This right provides the individual with the ability to get access to personal data that is being processed. This request provides the right for individuals to see or view their own personal data, as well as to request copies of the personal data.
Right to rectification	This right provides the individual with the ability to ask for modifications to personal data in case the individual believes that it is not up to date or accurate.
Right to withdraw consent	This right provides the individual with the ability to withdraw a previously given consent for processing of personal data for a purpose. The request would then require stopping the processing of personal data that was based on the consent provided earlier.

Right to object	This right provides the individual with the ability to object to the processing of their personal data. Normally, this would be the same as the right to withdraw consent if consent was appropriately requested and no processing other than legitimate purposes is being conducted. However, a specific scenario would be when a customer asks that their personal data should not be processed for certain purposes while a legal dispute is ongoing in court.
Right to object to automated processing	This right provides the individual with the ability to object to a decision based on automated processing. Using this right, a customer may ask for this request (for instance, a loan request) to be reviewed manually, because of the belief that automated processing of the loan may not consider the unique situation of the customer.
Right to be forgotten	Also known as right to erasure, this right provides the individual with the ability to ask for the deletion of their data. This will generally apply to situations where a customer relationship has ended. It is important to note that this is not an absolute right and depends on your retention schedule and retention period in line with other applicable laws.
Right for data portability	This right provides the individual with the ability to ask for transfer of his or her personal data. As part of such request, the individual may ask for their personal data to be provided back or transferred to another controller. When doing so, the personal data must be provided or transferred in a machine-readable electronic format.

Privacy risk	The term “privacy risk” means potential adverse consequences to individuals and society arising from the processing of personal data, including, but not limited to: 1. Direct or indirect financial loss or economic harm; 2. Physical harm; 3. Psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma; 4. Significant inconvenience or expenditure of time; 5. Adverse outcomes or decisions with respect to an individual’s eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services; 6. Stigmatization or reputational harm; 7. Disruption and intrusion from unwanted commercial communications or contacts; 8. Price discrimination; 9. Effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relate, that are nevertheless reasonably foreseeable, contemplated by, or expected by the covered entity assessing privacy risk, that significantly: A. Alters that individual’s experiences; B. Limits that individual’s choices; C. Influences that individual’s responses; or D. Predetermines results; or 10. Other adverse consequences that affect an individual’s private life, including private family matters, actions and communications within an individual’s home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected or used. 11. Other potential adverse consequences, consistent with the provisions of this section, as determined by the Commission and promulgated through a rule.
Risk of individual privacy harms	The likelihood that individuals will experience harm or problems resulting from personal data collection and processing
Risk of equity, disparate community impact	The likelihood that specific groups will experience harm or problems resulting from the collection of multiple sources of personal data and their processing.

Risk of political, reputation & image issues	The likelihood that collection or processing of private data may result in harm on professional or personal relationships, harm in reputation or image.
Risk of city business, quality & infrastructure issues	The likelihood that the collection or processing of private data may impact or expose city relationships, agreements, or any other contract, or the quality of those businesses, or built infrastructure
Risk of legal & regulatory issues	The likelihood of any violation of existing laws or regulations by the collection or processing of private information
Risk of financial Impact	The likelihood that ongoing costs in management, collection or processing of private data may become financially inviable or present costs that may not be considered