Apricot360

Case management system

Privacy Impact and Risk Analysis

FINAL Version.

Smart City PDX

December 14, 2023

PRIVACY ANALYSIS REPORT

City of Portland Privacy Toolkit

WHAT IS THE PRIVACY 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 of risks identified and the impacts on civil liberties or potential harm in communities.

In the interests of transparency about 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 AN PRIVACY IMPACT ANALYSIS RECOMMENDED?

A PIA is recommended when:

- 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.

HOW TO COMPLETE THIS DOCUMENT?

City staff complete two documents:

- *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: (1) Individual Privacy Harms; (2) Equity, Disparate Community Impact; (3) Political, Reputation & Image; (4) City Business, Quality & Infrastructure; (5) Legal & Regulatory; and, (6) Financial Impact. Then compares risks to the likelihood of happening to create a single risk measure based on the worst case scenario.

Executive summary

Apricot360 is a data entry, case management, and reporting tool for people who have experienced gun violence and who are referred by the Portland Police Bureau to the violence prevention program. The Office of Violence Prevention (OVP) will use it to replace current data management software used by service providers in the program.

The risk identified in the worst-case scenario (Risk 1.4) is **HIGH** and relates to the potential for disclosure of sensitive information in response to public records requests. However, this high risk can be mitigated by first informing all the applicants and contractors on how to **collect only the minimum and required information for the services they provide**. Some individuals may be requesting a specific public records exemption due to the danger of gun violence to them.

Some other risks, particularly those linked to data breaches, can be prevented if contractors are trained and follow the City's information protection and cybersecurity standards. Support can be requested from the Information Security team at the Bureau of Technology Services.

Risks connected to using the personal information from individuals for purposes other than those specified can be reduced by creating clear supervisory chains and protocols, including periodic audits, and limiting the ability to edit fields or downloading the data from the vendor's site. Audits should include data management, editing, sharing, reporting, and destruction of information.

The collection of unnecessary sensitive or personal information increases risks and city infrastructure required to properly protect it. Data minimization for a well-defined purpose is part of the City's privacy and information principles. This principle is very useful in this application.

We recommend the team plan periodic, as appropriate, public information releases on how effective the use of Apricot360 has improved operations, including metrics on program effectiveness. Further privacy checks need to be done to ensure that no personal or sensitive information is released in public reports and audits. These actions can increase public trust in the information platform and the collective of organizations that use it.

This assessment was completed on October 23, 2023.

Privacy Impact Analysis

Purposes of the technology, project, data sharing or application

The purposes are data entry, case management, and reporting for people who have experienced gun violence and are referred by the Portland Police Bureau to the violence prevention program. Apricot360 will replace data management software currently used by several community-based organizations (CBOs) contracted through the Office of Violence Prevention (OVP). The software brings better accessibility and enhanced functionality, and it will eliminate redundancies currently encountered while managing data on clients in Intensive Case Management and the associated reporting of data to Bureau (OVP).

This program by the Community Safety Division tracks up to 18 months for individuals referred by Portland Police Bureau to community-based providers. These individuals are people at risk of becoming perpetrators or victims of shootings. The program helps to find treatment, therapy, and housing.

The Office of Violence Prevention is the keeper of this information.
Apricot will (not intended as an exhaustive list):

- Eliminate reliance on paper forms for intake and case management.
- Automate much of the data reporting required by Bureau of CBOs, saving significant work hours and money in the process.
- Protect client personally identifiable information (PII) throughout the process.

Name of the entity owner of the application and website

Bonterra Technologies, Social Solutions. https://www.socialsolutions.com/products/apricot-360/

Type of Organization

Private

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

Personally Identifiable Information: name, address, birthdate, email, phone number. Additional sensitive information includes probation or parole status, safety concerns, substance use, gang affiliation, etc.

Contractors using Apricot360 will share business information and a list of case managers with the City. This information will be used to create internal accounts in Apricot360.

Contractors manage cases independently from Apricot360 and the City won't be able to see case or client information.

The City, either directly or through a designated representative, may conduct financial and performance audits of the billings and Products or Services at any time during the Contract and during the records retention period.

The City may examine, audit, and copy Contractor's books, documents, papers, and records relating to this Contract at any time during the records retention period.

How personal data is collected.

Data is obtained in-person from clients' computers or mobile devices. The vendor may include cookies and other mechanisms to track devices, browsers, and navigation from the interaction with the platform.

Who can access the data.

Each Contractor has access only to its own clients. Access to PII will be limited to the case managers of a particular contractor. The City can access only aggregated, anonymous data.

Purposes the data is used for.

The data will be used for client management by contractors, record of services provided, recording ARPA-mandated data, reporting data to City (anonymized)

Where the data is stored.

Data is stored on vendor-owned cloud servers.

How data is shared.

Apricot will be configured to send automatic reports to the OVP Program Manager. No sharing of data will be available among contractors using the system.

Portland Police Bureau shares information in referral that include name; date of birth; address; phone number; parent's or guardian's name & phone #, if the person is a minor; circumstances of police contact; and reason for referral. This information is not necessarily shared in Apricot360.

Contractors use the fields shared in Apricot360 for their case management system.

How long is the data stored?

The retention regime for these records is a minimum of six years. Contractor shall maintain current financial records in accordance with Generally Accepted Accounting Principles (GAAP). Contractor agrees to maintain and retain all financial records, supporting documents, statistical records and all other records pertinent to this Contract during the Term of this Contract and for a minimum of six (6) years after the expiration or termination date of this Contract or until the resolution of all audit questions or claims, whichever is longer.

Effectiveness

Data collected fulfills the purpose of the project. However, there is limited opportunity for privacy protection, particularly concerning sensitive personal information could be made public in cases of high public interest.

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

Fields collected from individual cases are required to manage each specific case properly. Individual privacy rights are limited to basic information protection. Individuals can correct their information by submitting requests directly to the contractors.

The City will regularly collect only aggregated data. No personal information will be transferred to the City directly. However, contractors will need to make sure that information is protected on their end.

Privacy safeguards

User definitions by the vendor

Customers

Representatives of prospective and existing *City contractors*. *Contractors provide direct services to individuals.*

- A representative of an organization that uses Network for Good to manage donations
- A representative of a public sector agency who uses Social Solutions to measure the impact of a community engagement project

Vendor has direct relationship with Customers.

Customer End Users

Individuals who are referred to the program become the contractors' users. The vendor defines them as 'Customer End Users'.

Vendor processes the personal information of Customer End Users pursuant to agreements with Customers – as a "services provider" or "processor."

How information is used by the vendor.

On behalf of the Customers, the vendor uses personal information to:

- Enable Customers to recruit and engage with vendor Users.
- Provide Customers with information relating to products, events, or other business information.
- Enable Customer End Users to complete transactions and make donations through the Services.
- Communicate with Customers and Customer End Users about these services and the City's account, including by sending announcements, updates, security alerts, and support and administrative messages.
- Provide support, and respond to requests, questions, and feedback.
- Provide marketing and advertising on behalf of Customers, including interest-based online advertising; and
- Build donor profiles for Customers' internal use through the Social Matching Feature. As directed by the Customers the vendor provides users with Customers' email contact lists by appending Customer End Users' email addresses with social media account information that the vendor obtains from third-party data providers.

Opting out data sharing to third parties

Vendor offers opt out of data sharing among Bonterra affiliates.

General privacy rights

The vendor offers some privacy rights. Customers have the right to submit requests about personal information, depending on location and the nature of interactions with Services:

- Information about how the vendor has collected and used personal information.
- Access to a copy of the personal information that the vendor has collected about the customer.
- Correction of personal information that is inaccurate or out of date.
- Deletion of personal information that is no longer needed to provide the services or for other lawful purposes.
- Opt out of the processing or sharing of personal information for targeted advertising.
- Opt out of the processing or sharing of personal information for targeted advertising.
- Appeal a denial of personal information request by contacting us as set out below.
- Additional rights, such as to object to and request that the vendor restricts the use of personal information.
- To make privacy-related requests contact vendor at privacy@bonterratech.com.

Retention.
The vendor retains personal information for as long as appropriate to fulfill the purposes for which the vendor collected it, including for the purposes of satisfying any legal, accounting, or reporting requirements, to establish or defend legal claims, or for fraud prevention purposes.

Cookies.
The vendor's platform may use cookies and other mechanisms to track what type of computer or mobile device is used, navigation, and user behavior tracking.

Security and Personal Data Breaches
The vendor will implement technical and organizational measures to protect Personal Data from Personal Data Breaches, such as:

a) encryption of Personal Data.
b) measures to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing.
c) measures to detect Personal Data Breaches in a timely manner.
d) measures to restore the availability and access to Personal Data in a timely manner in the event of an incident.
e) Processes for regularly testing, assessing, and evaluating the effectiveness of the security measures.

Vendor offers a data processing assessment document: https://assets.website-files.com/62013994e28a1f73b48f5c10/63c6e57b42b45ea8340c4397_Bonterra%20-%20Data%20Processing%20Addendum%20DPA%20Template.pdf

Open source

No

AI/ML claims

No

Privacy Policy

Vendor privacy policy https://www.bonterratech.com/privacy-policy
https://www.socialsolutions.com/legal/terms-of-service/
https://www.socialsolutions.com/legal/acceptable-use-policy/
data processing addendum: https://assets.website-files.com/62013994e28a1f73b48f5c10/63c6e57b42b45ea8340c4397_Bonterra%20-%20Data%20Processing%20Addendum%20DPA%20Template.pdf

Portland Privacy Principles

Data Utility

The City collects information that helps to determine what contractor and services are more adequate for each case management. The information collected by the City is the minimum required for the purpose of this program.

Full life cycle stewardship

Data life cycle includes contractors that may be collecting information from other sources, including clinics or other case management systems. The City starts the process by referrals received from Portland Police Bureau and connecting each case to these contractors. Contractors only have access to their individual cases, and they are responsible for managing them. Information protection is done using the Apricot360 platform. All the interactions with data are logged and can be audited if required.

Transparency and accountability

Aggregated data will be made open and publicly available by the City. This application would benefit from a clear set of performance metrics based on service level and data use effectiveness. Also, management of information in a privacy breach event is not defined. Actions triggered by a privacy breach on the contractors' side should include accountability and mitigation actions. An oversight strategy should include data audits to contractors and subcontractors will limit the risks of data breaches.

Ethical and non-discriminatory use of data

The City has an ethical obligation to protect the sensitive information it collects via independent contractors with the goal of providing better and more effective case management. The level of sensitivity is kept as low as possible to minimize risks and harm to individuals in cases of data breaches or potential abuses.

Data openness

Only aggregated data will be made accessible. Sensitive and private information will be kept separated and managed by independent contractors handling individual cases.

Equitable data management

The system will be used for all individuals, independently of their race, ethnicity, or social status.

Automated Decision Systems

Not applicable. No Automated decisions are made within this system.

Consent

No consent in data collection. Some information is taken directly from existing records.

Privacy Impact Risk Severity Assessment

WORST CASE SCENARIO	HIGH

1. Individual Privacy Harms

1.1 Risk of major data breach.

Risk level: **High** Risk likelihood: **Possible**	Total Risk level: **Medium**

Description of Impact:

Very sensitive information is collected by this program, including personal information, risk of individual violence or retaliation, history or recovery, and locations and addresses of contacts. This information may put individuals in danger.

Comments and mitigation:

A major data breach can be derived from loss of a device with unencrypted data, unauthorized copies of sensitive information, or cyberattacks. The City needs to inform and train all staff involved in sensitive information management on how to protect it properly and identify serious threats and risks.

Supervisors need to perform periodic verification of management of sensitive information, including reviewing Apricot360's activity logs.

The City needs to schedule audits, both internal and those performed by neutral and certified third parties. Periodic reports informing the public need to be planned and included in budgets.

1.2 Risk of privacy breach by contractors.

Risk level: **High** Risk likelihood: **Possible**	Total Risk level: **Medium**

Description of Impact:

The risk is that contractors could obtain additional information from referred individuals. This new information may contain additional sensitive information. If a data breach happens, it may impact those in danger of gunshot violence and create deep impacts to the services that the City may be able to offer in the future.

Comments and mitigation:

Contractors bear great responsibility to steward sensitive information on behalf of the City. The effectiveness of this program depends on the quality and trust that people from violent and traumatic situations are providing.

Contractors should follow City standards on information protection, including cybersecurity, data encryption, and best practices in data management. Their staff need proper training and access to certified personnel in charge of assisting with these implementations and supervision.

1.3 Risk of unnecessarily collecting sensitive information.

Risk level: **Medium** Risk likelihood: **Possible**	Total Risk level: **Medium**

Description of Impact:

Collecting sensitive information for which the City has no need will increase risks and potential negative impacts to referred individuals.

Comments and mitigation:

After an assessment period, it is important to review the effectiveness of information collected, particularly sensitive information. Collected information needs to bring value to the program and the people impacted by it. It also needs to be connected to specific aspects of the program.

Information that is not necessary or outside of the scope of the program should be removed.

1.4 Risk of releasing sensitive information via a public records request.

Risk level: **High** Risk likelihood: **Likely**	Total Risk level: **High**

Description of Impact:

The program collects specific personally identifiable information (PII) from those individuals referred by Portland Police Bureau to this program. This information includes client first and last names, date of birth, email, phone number, affiliation, program enrollment date, probation or parole status, presence of ID documents, education information, employment status, housing status, substance use, health information, information on whether the client has been shot in the last 6 months, and additional notes.

Comments and mitigation:

The information collected by the program may be subject to disclosure under Oregon's public records statutes.

To mitigate this risk, the Bureau should:

- Minimize the collection of sensitive information and only display those fields that are required to provide the service or assure the quality and success of the program connected to an approved performance measure.
- Add a data protection disclosure to the collection of information from individuals who are victims or are at risk of gun violence.

- Add a data protection disclosure to any data-sharing agreement that may involve an individual's sensitive information.

Forms collecting information directly from individuals should include a warning such as the following:

> ***Complete information, including contact and other personal information, may be necessary to fulfill the services of this program. Please note that your information is confidential and, to the extent possible under the law, will not be provided to the public.***

Reducing the number of sensitive fields, working with contractors to assure information protection measures, and informing individuals about these risks, may reduce this risk to a medium level.

2. Equity, Disparate Community Impact

2.1 Specific privacy risks on vulnerable groups.

Risk level: **Medium**	Total Risk level: **Medium**
Risk likelihood: **Possible**	

Description of Impact:

The risk is that certain groups that may be referred by this program could have specific privacy vulnerabilities and protections. These groups may include minors, women, people with disabilities, veterans, and the elderly.

Comments and mitigation:

2.2 Risk of escalating community violence due to a privacy breach or unauthorized information release.

Risk level: **High**	Total Risk level: **Medium**
Risk likelihood: **Unlikely**	

Description of Impact:

The risk is that access to unauthorized released personal information of individuals at danger of being shot or under threat could trigger acts of violence in the community.

Comments and mitigation:

In case of an unauthorized released of information, the best strategy is to act promptly and responsibly. Individuals impacted by the information breach need to be informed as soon as possible and corrective and mitigating measures need to be taken as soon as possible.

Further transparency and accountability measures need to be taken according to the law, existing regulations, and best practices adopted by the City.

3. Political, Reputation & Image

3.1 Political risk due to impacts on the City's public trust.

Risk level: **High**	Total Risk level: **Medium**
Risk likelihood: **Unlikely**	

Description of Impact:

The risk is that the City's public trust could be highly impacted by any issue derived from a privacy data breach ending in harm to any individual or group referred to this program.

Comments and mitigation:

A City privacy risk can impact public trust of services involving sensitive information. We recommend ensuring all the personnel involved in this system have received the latest cybersecurity and information protection training. All sensitive information should only be accessed temporarily and any trace of sensitive and personally-identifiable information on any transition device should be deleted.

Supervisors need to be trained in data management best practices and information protection, including privacy breaches and incident management. They should also understand supervisory features on Apricot360, not only for City users but also for external users.

Plan periodic audits and internal and public reporting releases.

Prepare proper communications and reporting of outcomes and performance measures of this program and release them periodically. A monthly or bimonthly release can build meaningful trends and narratives that help public trust.

3.2 Risk of damaging reputation of contractors due to privacy issues.

Risk level: **High**	Total Risk level: **Medium**
Risk likelihood: **Possible**	

Description of Impact:

The risk is that contractors could face issues of public trust due to privacy and information protection issues. This can include privacy breaches, unprepared or untrained staff managing sensitive and personal information, and lack of digital infrastructure, including cybersecurity and sensitive information protections.

Comments and mitigation:

The City needs to ensure that digital infrastructure of contractors follows City standards on information protection, including cybersecurity.

Contractors' staff need to be properly trained to identify sensitive information and to ensure they understand the procedures to protect the information properly.

The contractor should be responsible for protecting computers, laptops, and other devices that collect, manage, process, and dispose properly sensitive information.

The contractor should also ensure proper internal oversight and supervision of data operations, including data encryption and decryption keys management.

3.3 Risk of using this information for other purposes.

Risk level: **High**	Total Risk level: **Medium**
Risk likelihood: **Unlikely**	

Description of Impact:

The risk is that information collected through this program and system could be used for other purposes, such as criminal investigations, identifying the whereabouts of a specific individual, data mining for other purposes outside the scope of this project, or forecasting gunshot incidents. These unspecified uses can impact the reputation of these services and program.

Comments and mitigation:

Avoid uses of this information, particularly sensitive information, that are out of the scope of this program.

If required, request proper authorization by the bureau director and inform the public. If a third party is requesting access to information for other purposes, ask for authorization and communicate to the public in a timely form.

Certain requests of information involving specific individuals must be denied and only aggregated and anonymized data should be provided.

If academic researchers request information, develop a proper information sharing agreement and work with City Attorneys to define proper information protection measures and clauses that protect the City and individuals from unauthorized releases or uses, and information safeguards.

4. City Business, Quality & Infrastructure

4.1 Risk of mismanagement by contractors.

Risk level: **High** Risk likelihood: **Possible**	Total Risk level: **Medium**

Description of Impact:

The risk is that the contractor's processes and information system could allow misuse, create vulnerabilities, unauthorized copies of information, or potentially releasing sensitive information on purpose.

Co**mments and mitigation:**

Prepare clear and effective documentation and information for onboarding contractors to the City's information protection best practices.

Plan frequent check-in meetings with contractors' supervisors and ensure that all their staff, including new ones, have been trained in managing sensitive information and using Apricot360 properly.

Add language that ensures clear understanding by contractors of privacy and information protection, including data breach notifications, and collaboration in incident management.

4.2 Risk of data misalignment.

Risk level: **Medium** Risk likelihood: **Possible**	Total Risk level: **Medium**

Description of Impact:

There is a risk of data misalignment when two entities use different data to represent the same thing. This can happen if contractors or any other stakeholder updates information without updating all the system.

Comments and mitigation:

Make sure that any updates on the contractors' systems are also updated in Apricot360.

Managing multiple contractors' systems may create additional information risks. Collaborate with the contractor's IT staff to make sure the latest information required by the City is transferred timely and accurately.

4.3 Risk of jeopardizing proper privacy protections by collecting unnecessary information.

Risk level: **High** Risk likelihood: **Possible**	Total Risk level: **Medium**

Description of Impact:

There is a risk of collecting unnecessary data that may make it more difficult to implement proper oversight and performance metrics of these case management services. Unnecessary information may also increase risks and impacts in privacy data breaches and require more protection of sensitive information. Some of that data could be about the contractor's performance, while some other information could measure the program effectiveness and include additional sensitive information that was not yet considered.

Comments and mitigation:

As the program matures, new issues may arise. Include annual versioning control revisions of the information architecture. Make sure revised and effective performance metrics and oversight strategies are developed and implemented.

Some performance measures may be customized to specific contractors due to the nature of their operations or information system. Make sure that the management of those information systems include updated privacy and information protection systems.

IT systems upgrades may change certain configurations. Constant communications with contractors can make the integrated information system more robust.

5. Legal & Regulatory

5.1 Risk of legal action against the City or contractors due to privacy breaches.

Risk level: **Medium** Risk likelihood: **Unlikely**	Total Risk level: **Medium**

Description of Impact:

The risk is that a data breach, particularly one that ends in loss of life or property damage, could create legal liability for the City if the breach was due to mismanagement or lack of training or oversight of City staff or contractor's staff.

Co**mments and mitigation:**

Make sure to follow the Oregon data and security breach laws (ORS 646A.604) and prepare a data breach incident plan. It is particularly important to focus on sensitive information from at-risk individuals.

Connect with the City's information security team to prepare this plan.

Ensure that all personnel (City, contractors, and subcontractors) are trained and understand how to manage sensitive information.

Supervisors need to schedule time for oversight and revision of log histories and communications with contractors' IT teams to make sure no incidents have appeared. Keep documentation of those meetings.

6. Financial Impact

6.1 Financial risk of a compensation claim due to damage created by privacy breaches.

Risk level: **Medium** Risk likelihood: **Possible**	Total Risk level: **Medium**

Description of Impact:

The risk is that a privacy breach from any of the stakeholders, including contractors, could result in claims against the City due to impacts or damage to individuals or organizations.

Co**mments and mitigation:**

The City may receive claims for damage compensation after a data breach has occurred. Work with City attorneys and the City's information security team to service these claims.

6.2 Financial risks to third parties due to additional digital infrastructure not considered in this project.

Risk level: **Medium** Risk likelihood: **Possible**	Total Risk level: **Medium**

Description of Impact:

Full life cycle protection requires that all participants in data management implement data protection measures across organizations. The main risks of a breach or attack comes from the weakest link in the information chain.

Comments and mitigation:

Some contractors may have trouble fulfilling the information protection requirements of the City. Work with them to try to mitigate the highest risks during the transition or the implementation of these IT infrastructure and procedures.

Work with the City's information security team to support contractors' and subcontractors' implementation of these IT requirements.

6.3 Risk of failing to report a data breach.

Risk level: **Medium**	Total Risk level: **Low**
Risk likelihood: **Unlikely**	

Description of Impact:

There could be a financial penalty if a data breach is not reported.

Comments and mitigation:

Report data breaches immediately and work with the City's information security office. Determine the level of impacts and develop a proportional action plan for remediation and mitigation.

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	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 to 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 identity cards would 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 believe 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 the 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