2025 Privacy Impact Assessment

Verkada Guest

SPD

10/30/2025

Seattle Information Technology

Contents

Seattle Information Technology

Privacy Impact Assessment Overview

What is a Privacy Impact Assessment?

A Privacy Impact Assessment ("PIA") is an analysis of how personal data is gathered, processed, and used for a particular program, project, data initiative, or technology implementation (the terms may collectively be referred to hereafter as "effort"). The PIA asks questions about the collection, use, sharing, security, and access of data involved in a City department effort. It also requests information about policies, training, and documentation that govern the use of the data and any associated technology. The PIA responses are used to determine privacy risks and mitigation measures to reduce those risks. To ensure transparency about personal data collection and management, the City of Seattle has committed to publishing all PIAs on an outward-facing website for public access.

When is a PIA required?

A PIA may be required when a project, program, or other data processing activity has been flagged through the privacy review process as having a high privacy risk.

How to complete this document?

As department staff complete the document, they should keep the following in mind.

- Department Subject Matter Experts (SME) are responsible for providing responses to the questions. *Please do not edit the questions or question descriptions that are part of the template.*
- All content in this report will eventually be published to the public. Therefore, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written principally using non-technical language to ensure they are understood by audiences unfamiliar with the topic.

Seattle Information Technology

1.0 Overview

1.1 Description: Please describe the effort.

Include high level descriptions of any technology and its intended use, the data collected or processed, and all third parties involved in the effort.

Function: visitor check-in, triage, visitor notification to staff using Active Directory.

Verkada Guest is a visitor management system that provides guest check in solutions to strengthen building security. It will be used at the SPD HQ for the check in and triage of SPD visitors. Verkada's check-in solution can be used to streamline visitor or personnel tracking at a facility. For example, when someone arrives on site—like a contractor, staff member, or community guest—they can check in using a tablet or mobile device at the entrance.

They enter their name, purpose of visit, and who they're meeting, and the system can, if visitors elect to, capture a photo and notify the host. This data is logged in real time, integrated with one camera, allowing for easy audits, enhanced safety, and clear visibility into who was present and when.

Enhances front desk security and ensure we are in compliance with regulatory requirements & reduces manual visitor tracking and administrative overhead.

1.2 Business Need: What business need/problem does this effort address?

Please describe why the department is undertaking this effort.

This technology is replacing Lobbyguard.

The purpose is to streamline visitor check-in.

1.3 Benefits: What are the anticipated benefits of this effort, and how does it relate to departmental and/or City mission?

What is the intended outcome, goal, or benefit? Please provide any data or research demonstrating the anticipated benefits of the effort (e.g. academic studies, etc.).

Speed. The paper check-in process doesn't provide visibility into SPD visitor trends and causes congestion at the reception desk. Using a self-registration kiosk at the entrance provides a streamlined way to manage visitor entry while keeping the reception area clear and moving quickly. In a matter of seconds, visitors can scan their driver's license or other ID or enter details into the kiosk to register their visit, relieving the burden on the desk officer and providing an improved experience for visitors. Pre-registration allows staff to schedule their upcoming visitors to expedite the check-in process.

Security. A digital visitor system improves security by providing a digital record of visitors on-site. The first step in making sure everyone on your premises is safe in an emergency is knowing exactly who's on your premises. With a visitor management system, SPD will have access to reports to identify all on-site visitors both in real time and retroactively. Printed badges let staff easily recognize visitors and verify they are in the correct area. By using a digital visitor management system, SPD will collect and store details of visitors for a limited period. Because of this, SPD will need to gain consent from the individual

to do so. This can be achieved by ensuring that the individual reads and understands the privacy policy and by moving forward in the process and receiving a badge they are acknowledging that they agree with the privacy policy and conditions of storage and give consent for their data to be stored in the system.

1.4 Technology Details: Describe all technologies that support or will be used as part of the effort.

What systems interact with the data involved in this effort? This includes hardware and software throughout the data lifecycle (e.g. creation, collection, use, storage, disclosure, and destruction). Describe, by name and functionality, all technologies associated with the effort. For example: high-level Microsoft Forms to collect the data, Microsoft Excel to extract the data.

Verkada Guest is a visitor management system that provides guest check in solutions to strengthen building security. It will be used at the SPD HQ for the check-in and triage of SPD visitors. Verkada's check-in solution can be used to streamline visitor or personnel tracking at the facility. For example, when someone arrives on site—like a contractor, staff member, or community guest, they can check in using a tablet at the entrance. They enter their name, purpose of visit, and who they're meeting, and the system can capture a photo and notify the host. This data is logged in real time, integrated with one camera, allowing for easy audits, enhanced safety, and clear visibility into who was present and when.

The solution will integrate with Active Directory to alert staff that they have a visitor.

1.5 Scope of Involvement & Use: Who is involved in the implementation or use of the technology, project, and associated data?

For example, what other departments, if any, are involved? Are external partners (e.g. community-based organizations) or vendors/consultants involved?

This system was installed and is maintained by SPD staff. Designated Seattle IT staff are also involved in supporting and maintaining the system.

2.0 Data Details & Collection Practices

2.1 Data Subjects: Whose data will be collected or processed as part of this effort?

Please provide all categories of data subjects (e.g., members of the public, City employees, contractors, etc.) as well as any sub-populations that might be involved (e.g., children, older adults/elderly, incarcerated or formerly incarcerated persons, unhoused persons, etc.)

Data subjects will be people who visit SPD HQ and choose to use the Verkada system. There are multiple options for entering HQ ; use of Verkada is optional.

2.2 Data Fields: What are the data fields and data types that are involved in this effort?

Please describe all data collected, stored, generated, analyzed, used, and/or shared, etc.

If a person chooses, the system will scan the Driver's License and automatically capture the Date of Birth and Name from the ID into the appropriate fields.

If the person does not have an ID, they will be able to sign in manually. (Input their name, DOB, and purpose of the visit.)

If a visitor opts in, the photo will be captured in addition to the name and date of birth.

We will also create a workflow that does not require a photo (opt out).

Name of the employee the visitor came to meet will also be collected.

2.3 Data Collection: How is the data collected for this effort? What are the data sources for the data used or processed as part of this effort?

Please describe the methods of data collection (e.g., first-party collection which is collection directly from an individual; third-party collection, which is collection through another entity, etc.). Also include the mechanism by which the data is collected (e.g., online form/survey, data purchase, data shared/provided by another department, etc.).

First-party collection – the system will scan the Driver's License and automatically capture the date of birth and name from the ID into the appropriate fields.

If the person does not have an ID, they will be able to sign in manually. (Input their name, date of birth, and purpose of the visit.)

The photo will be captured in addition to the name and date of birth.

2.4 Data Flow: Describe how data collected flows through the data lifecycle including the assets used to store and process the data. ("Assets" are things that support the information-related activities, such as software systems, appliances, databases, etc.)

In other words, after data is obtained, where will it go? Where will it spend most of its time? Will it stay put, or will it go somewhere else?

The data will be stored in the software's cloud and will be primarily accessed by the officers manning the front desk.

Data can be accessed for public disclosure requests or during a facility emergency to see who is in the building.

2.5 Notice: At the point of data collection, how are individuals notified about the City's use, sharing, and disclosure of their personal data?

Please include all methods, processes, or mechanisms for notification. This may include the City's standard disclosure, use, and sharing notice.

Yes, this will be displayed on the screen if people choose to use Verkada and they will need to opt in/acknowledge. Additionally, visitors are able to opt out of using Verkada.

Seattle Information Technology

3.0 Data Use & Processing

3.1 Authorized Data Uses: What are the authorized uses of the data associated with this effort?

In addition to describing all authorized uses of the data, list any data use limitations and unauthorized data uses.

Data is sent to staff identified by the system as able to receive visitors via email and optionally text, notifying them that their visitor has arrived. All SPD employees are backgrounded, and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems, including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy

Data can be accessed for public disclosure requests or during a facility emergency to see who is in the building.

3.2 Authorized Technology Uses: What are the authorized use cases for the technology associated with this effort? How may the technology be used?

In addition to describing all authorized use cases for the technology, list any technology use limitations and unauthorized technology uses.

This solution is a check-in solution that is replacing LobbyGuard. It is authorized only for visitor check-in at SPD HQ.

3.3 Use & Management Policies: What policies (City or department-specific) apply to the use and management of the data *and* technology (if different than the data) associated with this effort?

Please name and describe all applicable policies.

All information must be gathered and recorded in a manner that is consistent with SPD Policy 6.060, such that it does not reasonably infringe upon "individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech, press, association, and assembly; liberty of conscience the exercise of religion; the right to petition government for redress of grievances; and the right to privacy." All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

3.4 Data Processing & Analytics: Please describe how the data will be processed and analyzed in support of the intended business goal/outcome. Please include metrics.

Describe the scale of processing and analysis to the best of your ability, as well as whether analysis involves matching or combining datasets. Describe the fields required for joining, and the metrics the business will use for the analysis.

Data is sent to staff identified by the system as able to receive visitors via email and optionally text, notifying them that their visitor has arrived. All SPD employees are backgrounded, and access is

controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy

4.0 Legal Scope & Compliance

4.1 Governing Laws: What laws, regulations, rules, or contracts govern (a) the data, (b) the data processing activities, (c) the data sharing?

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law. Data may be shared with outside entities in connection with criminal prosecutions:

• Seattle City Attorney's Office

• King County Prosecuting Attorney's Office

• King County Department of Public Defense

• Private Defense Attorneys

• Seattle Municipal Court

• King County Superior Court

• Similar entities where prosecution is in Federal or other State jurisdictions Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA").

SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050).

Individuals can access their own information by submitting a public disclosure request. Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

4.2 Compliance Measures: What are the compliance measures associated with the use of the technology or data? Who is involved with oversight of requirements defined in 4.1?

Please explain any departmental, City, and/or third-party oversight.

Access to the system is limited only to trained staff, authorized SPD administrators, and authorized Seattle City IT administrators.

4.3 Records Production Compliance: How is the data and/or associated records (e.g., reports, derivatives, etc.) retrievable in support of public disclosure requirements?

Please describe the method and process for extracting/retrieving/producing the data.

Logs can be accessed and downloaded from the system on demand/as needed. Retention periods are determined by City Clerk and will be applied to the solution.

5.0 Data Security, Protection, & Storage

5.1 Data Access: Who will have access to the data? Who will have access to the technology (if different than who has data access)?

Specific users identified designated as admins will have access to data and the technology.

5.2 Access Authorization: What processes are prerequisites to a user's access of the data or technology (e.g., user authentication, business approvals/sign-off, documentation, etc.)?

As part of your response, include who (by City title) is responsible for authorizing data access.

Users will log into the system using single sign-on, with select users being granted admin permissions by the department leads.

5.3 Secure Storage: Where will the data be stored, and what security measures are in place for the storage of the data?

Data will be stored in AWS cloud. This is set with role based access, single sign on and with only City credentials.

5.4 Auditability of Data Access & Data Processing: How will the department ensure that data access and data processing activities are logged and auditable?

This could be conducted manually (e.g., business process), by technology/technical functionality, or a combination of both.

The logs are stored automatically by the system and can be reviewed and accessed on demand.

6.0 Data Sharing & Disclosure

6.1 Data Sharing Partners: Which entities (internal and external to the City) will be data sharing partners, if any?

Please describe all parties that will have access to both the data and data derivatives (including other City departments).

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law. Data may be shared with outside entities in connection with criminal prosecutions:

• Seattle City Attorney's Office

• King County Prosecuting Attorney's Office

• King County Department of Public Defense

• Private Defense Attorneys

• Seattle Municipal Court

• King County Superior Court

• Similar entities where prosecution is in Federal or other State jurisdictions Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA").

SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050).

Individuals can access their own information by submitting a public disclosure request. Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

6.2 Purpose for Data Sharing: What is the purpose of sharing data with the identified parties in the context of this effort?

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

6.3 Sharing Restrictions: Describe any restrictions on data use and data access and identify the sources that impose those restrictions.

Data sharing agreements/contracts, department policies and procedures, department rules, laws, regulations, and other authorities may impose data restrictions.

SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050).

6.4 Agreement Updates: Please describe the process for reviewing and updating data sharing agreements.

Please describe the processes for initial development, agreement review, new uses of the data, and new access to the data (including internal and external to the City) as well as how often the agreement gets updated.

There is no expectation that access will change. However, if there are any changes to data collected or data practices with Verkada this PIA and other relevant documentation will be updated to reflect these changes.

6.5 Records of Data Disclosure: How are records that document data disclosure/sharing maintained by the department?

Please describe how these records are documented either by technical functionality or business practices/processes.

User logs will be stored by the system automatically and can be retrieved on as as-needed basis when requested by the PDR team.

7.0 Data Retention & Destruction

7.1 Data Retention: What are the record retention schedules that govern both the raw data and any derived outputs (e.g., analyses, reports, transformed/cleaned datasets)?

Entry logs (name, date of visit, and person being seen) is retained for 6 years.

Optional photo (opt in) will be retained for only 24 hours.

Optional guest ID optical character recognition (name and Date of birth) will be retained for only 24 hours.

Email to alert staff of visitor: will be deleted based on inbox retention. Verkada will delete the alert in 24 hours of sending.

7.2 Data Destruction: What mechanisms (technical or process-oriented) are in place to destroy improperly collected data?

The system collects specific data only. Data destruction for the optional photo and ID details is built into the system based on the 24 hour retention time limit.

7.3 Responsible Staff: Who is responsible for ensuring compliance with data retention and data destruction requirements?

Please respond with City title(s)/roles only.

The SPD Records manager. Information will automatically expire upon set retention. Only information being recorded is logs.

7.4 Purge Verification: What mechanisms (technical or process-oriented) are in place to ensure that data is properly destroyed after data retention periods have been met?

Automatic setting will ensure that the data is not retained beyond the appropriate retention schedule.

8.0 Privacy Principles, Risks, & Controls

The City's Privacy Program staff will help in completing this section.

8.1 Privacy Risks, Harms, Mitigations, & Controls: What privacy risks exist for the effort, and what are the potential impacts on Seattle residents and/or other data subjects?

What are the controls or mitigations that are in place to address these risks, and reduce the likelihood that unintended harms are realized?

Risk: Concern around biometric information collection/sharing through photo collection.

Mitigation: Photo is opt in and not retained. Clear and visible signage will serve to communicate opt-in as well as alternative sign in mechanism. **No facial recognition is used in this technology.**

Risk: Concern around sensitive data collection.

Mitigation: System is opt in. If visitors opt in, they do not have to have a photo taken. Information that is collected is visitor name, date of visit, and the person being visited. If photo is taken it is retained for 24 hours only and then automatically destroyed. Access to data is role based and audit log is available.

Risk: Sharing data with third parties can increase risk associated with a lack of control over the data. Concerns exist over access to system by third parties.

Mitigation: Data will be stored in AWS cloud. This is set with role-based access, single sign on and with only City credentials. No data will be shared with third parties outside what is defined above. Additionally, minimal information is retained as needed. Strict access controls are in place for the limited data that is retained.

Risk: Chilling effect: People entering the headquarters may fear over-surveillance and this may in turn dissuade them from seeking services (for example, if person is in abusive or dangerous home situation they may want to report but fear being filmed and this being publicly disclosable). Personal data elements collected on data subjects considered to be part of a vulnerable population present an increased and potentially disproportionate risk associated with individual privacy harms and confidentiality.

Mitigation: Participation with Verkada solution is completely optional and does not impact visitor experience (i.e. – no priority is given to those using Verkada over those who choose not to). Additionally, for individuals with safety concerns there are specific entrances that they can use that ensure their confidentiality and privacy.

If an individual opts-in to using Verkada, the retention of the data collected will be minimized to the greatest extent possible. Information that is collected is visitor name, date of visit, and the person being visited, this is retained for 6 years per City of Seattle retention policy. If photo is taken it is retained for 24 hours only and then automatically destroyed.

No information related to the intent of the visit to SPD is collected by the system.